Desktop Surveillance Help

Table of Contents

About **5**
What's New **6**
System Requirements **7**
Program structure **8**
Program Structure 8
Server Tray 9
Viewer Tray 9
About Viewer Tray 9
Tray Notifications Journal 9
Deployment and Administration **11**
About Program Installation 11
Installing/uninstalling/updating Desktop Surveillance Server 11
Installing Desktop Surveillance Server and Administrative Panel 11
Adding Server Executable to Windows Firewall 15
Updating Desktop Surveillance Server 23
Database Types Comparison 25
Uninstalling Desktop Surveillance Server and Administrative Panel 26
Installing/uninstalling/updating Desktop Surveillance Viewer 28
Installing CensorNet Desktop Surveillance Viewer 28
Updating the Desktop Surveillance Viewer 29
Uninstalling Desktop Surveillance Viewer 31
Installing/uninstalling/updating Desktop Surveillance Clients 34
About Desktop Surveillance Clients Installation 34
Client Installation prerequisites 34
Setting up Environment for Client Remote Installation 34
Disabling Simple File Sharing in Windows XP 35
Disabling Sharing Wizard in Windows 7 36
Checking System Services 36
Disabling Windows XP/Vista Firewall 37
Setting Up Windows 7/8 Firewall 39
Installing Desktop Surveillance Clients via Administrative Panel 42
Installing Clients via Installation Package 49
Updating the Desktop Surveillance Clients 51
Cloning a Virtual Machine with Installed Client 52
Uninstalling Clients 52
Licensing 55
General Licensing Information 55
About Subscription 56
Activating Serial Keys Online 56
Adding Activated Serial Keys Offline 57
Viewing License State 57
Deactivating Serial Keys 58
Desktop Surveillance Client License Management 58
Troubleshooting 60
Checking that the Client is Installed 60
Clients Installation Issues 62

Remote Client Installation Issues....63
Administrative Panel....64
Administrative Panel Properties....64
Administrative Panel interface....65
Administrative Panel Interface....65
Administrative Panel Options....67
Roles....67
About Roles....67
Assigning Roles to Users....68
Assigning Roles to User Groups....71
Unassigning Roles from Users/User Groups....73
Working with data....74
Moving Desktop Surveillance Server Database....74
Deleting Data....75
Shrinking Database....77
Alerts....78
About Alerts....78
Alerts management....79
Adding Alerts....79
Editing Alerts....79
Viewing Alerts....80
Deleting Alerts....81
Alert Parameters....82
Rules....83
Examples of Rules....84
Defining Alert Global Settings....85
Desktop Surveillance Client Configuration....87
Export....88
Viewer....89
Connecting/Disconnecting from Desktop Surveillance Server....89
Viewer interface....90
Viewer Interface....90
Panes....91
Main Menu....92
Search....93
About Searching....93
Quick Search....94
Parameterized Search....94
Parameterized Search Parameters....95
Saving Search Parameters....97
Restoring Search Parameters....99
Examples of Search Parameters....100
Viewing monitored data....101
Viewing Screen Captures....101
Viewing Live Sessions....102
Receiving Information on Alert Events....103
Reports....104
About Reports....104
Search Results Report....104

Session Activity Report 106
Exporting Video 107
Saving Screen Captures 108

About

Welcome to CensorNet Desktop Surveillance!

CensorNet Desktop Surveillance is an application that allows you to record the activity of the target computers with installed Clients and to view the screen captures from these computers in the form of video.

What's New

Desktop Surveillance v. 2.2 introduces the following changes:

- **Licensing process became easier and more user-friendly**. Now, you have to purchase serial keys and activate them via Internet. After this simple action, you'll be able to assign licenses to Clients for working with them. Offline activation is supported for users that don't have Internet on their Desktop Surveillance Server computer.
  NOTE: If you already have the licensed Desktop Surveillance, you need to receive new serial keys from your vendor and activate them.
- **The minimal screenshot color depth is 4 bit grayscale**. Screenshots created with such color depth require less space for storing (database size reduces by more than 20%) without information value loss.
- **Windows 8.1** support is added.
- **The Desktop Surveillance Remote Clients installation wizard is changed** to make Client installation process more transparent and allow a user to avoid possible problems.
- **Desktop Surveillance Client and Server logs are optimized.** Out-dated logs are automatically removed a computer. Client work is less noticeable to the user.
- **Desktop Surveillance performance is improved.** Desktop Surveillance Server and Viewer work quicker now.
- **The help file format has been changed to PDF**. Now, you can easily print a user manual.
- **Overall stability is improved**. Possible minor problems with processing large amounts of data are fixed.

System Requirements

Desktop Surveillance claims different system requirements for each of its components. Make sure your hardware and software meet the Desktop Surveillance system requirements to avoid possible component malfunctions.

Desktop Surveillance Server requirements:

- 2 GHz or higher CPU
- 1024Mb or more RAM
- 100 Mbit/s network adapter (1 Gbit/s is recommended)
- Microsoft Windows XP, Vista, 7 (any edition except Home), 8, 8.1; Microsoft Windows Server 2003, 2008, 2012. Both x86 and x64 platforms are supported.

Desktop Surveillance Viewer requirements:

- 2 GHz or higher CPU
- 1024Mb or more RAM
- 100 Mbit/s network adapter
- Microsoft Windows XP, Vista, 7, 8, 8.1; Windows Server 2003, 2008 and newer. Both x86 and x64 platforms are supported.

Desktop Surveillance Client requirements:

- 1 GHz or higher CPU
- 512 Mb or more RAM
- 100 Mbit/s network adapter
- Microsoft Windows XP, Vista, 7, 8, 8.1; Windows Server 2003, 2008 and newer. Both x86 and x64 platforms are supported.

NOTE: When Desktop Surveillance Client is installed to the terminal server, hardware requirements depend on the number of active user sessions and may increase drastically. For example, hardware requirements for Desktop Surveillance Client deployed on the terminal server hosting 10 active user sessions will be as follows:

- **Intel Core i3 or similar AMD CPU**
- **2048 Mb RAM**

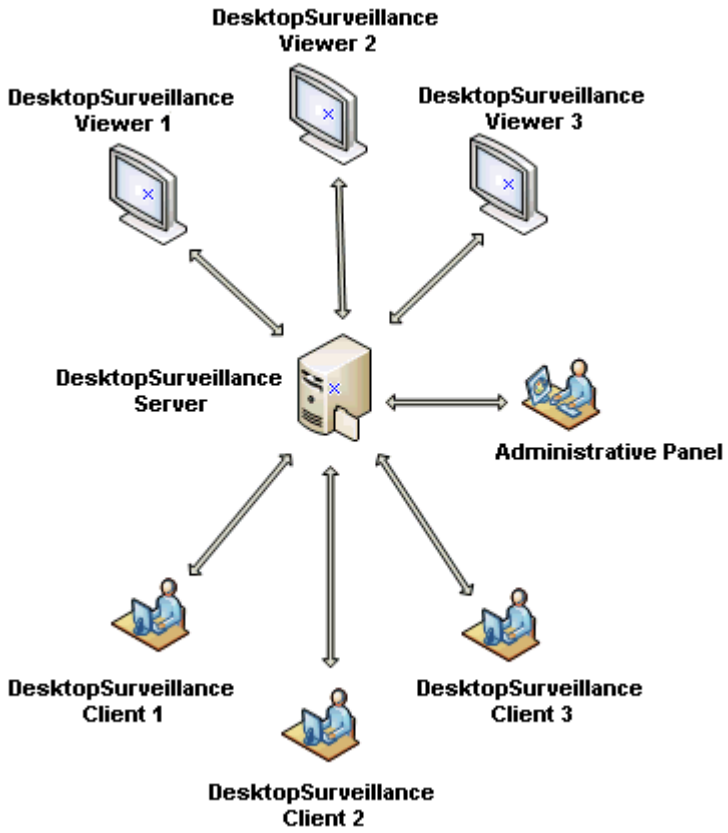
Program structure

Program Structure

CensorNet Desktop Surveillance is an application specially designed to control user activity remotely.

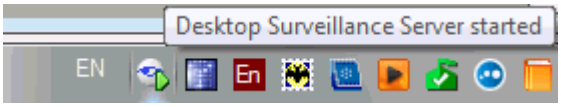
CensorNet Desktop Surveillance includes the following components:

- **Desktop Surveillance Administrative Panel:** Is the interface part of Desktop Surveillance Server used to manage the Desktop Surveillance system.
- **DesktopSurveillance Server:** It is the main part of the CensorNet Desktop Surveillance used for storing the screen captures and associated information received from the Clients. The work of the Server can be started or stopped via **Server tray**.
- **DesktopSurveillance Viewer**: This part of the CensorNet Desktop Surveillance provides a usable interface for quick viewing and analyzing of the screen captures received from the Clients. The alert monitoring function of the Viewer is accessible via **Viewer tray**.
- **DesktopSurveillance Clients:** Being installed on host computers, Clients create screen captures with certain quality and the defined frequency and send them to the server. Clients screen captures creation configuration can be managed through the CensorNet Desktop Surveillance Administrative Panel.



Server Tray

The Server Tray application informs you about the Desktop Surveillance state.



It also automatically restarts the Desktop Surveillance Server in case of its failure. The first three times the restart is performed automatically. The user is informed about the Server failure in the notification area. If the Server fails for the fourth time, it does not restart.

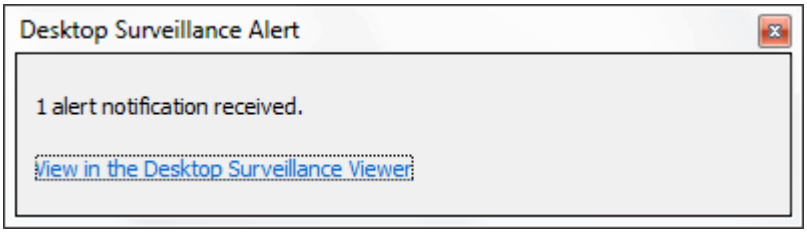
You can start/stop Desktop Surveillance Server or hide the tray icon from the notification area.

If you want to contact the Support, you need to collect the Server log (%PROGRAMFILES%\ CensorNet\Desktop Surveillance\Server\ ServerService.log) and attach it to the request.

Viewer Tray

About Viewer Tray

Desktop Surveillance Viewer Tray is a special utility that notifies the investigator about the alert events on the investigated computers. The alerts are displayed in the pop-up notifications from the Windows tray area. The notifications may be set up to be displayed immediately or with a delayed response in the **Alert Global Parameters** accessible from the **Administrative Panel**.



Left-click on the tray icon opens the latest notification in the **Viewer**.

Right-click on the tray icon opens the context menu. It contains the following options:

Disable/enable tray notification: Disables or enables the pop-up notifications from the Windows tray.

Open tray notifications journal: Opens the journal containing the records of the latest notifications on alerts on the investigated computers.

Stop viewer tray service: Terminates the work of the utility.

NOTE: To enable automatic launch of the Viewer Tray service at system startup, you need first to log in to the Viewer at least once.

Tray Notifications Journal

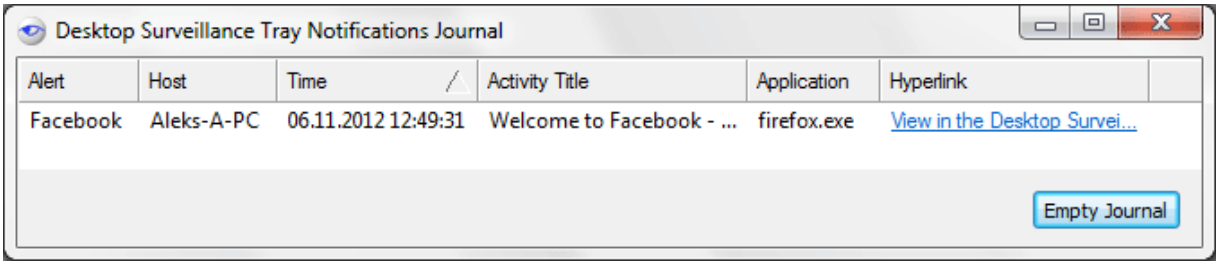
Tray Notifications Journal keeps the records of the latest alert notifications from the investigated computers. The maximum number of the records in the **Tray Notifications Journal** is defined by the investigator in the **Alert Global Settings** in the **DestopSurveillance Administrative Panel**. When it is reached, the latest records are removed from the journal. The records can be cleared by clicking the **Empty Journal** button.

NOTE: Information removed from the journal is not deleted from the database.

Information is displayed in the grid containing such columns:

- **Alert**: Displays the Alert name.
- **Host**: Displays the name of the computer on which the Alert event occurred.
- **Time**: Displays the time when the Alert event occurred on the investigated computer.
- **Activity Title**: Displays the name that appeared in the title of a window when the Alert event occurred on the investigated computer.
- **Application**: Displays the name of the started application on the investigated computer when the Alert event occurred on the investigated computer.
- **Hyperlink**: This column contains the link to the Alert screen capture in the **Desktop Surveillance Viewer**. Left-click on it automatically launches the **Viewer** and takes the investigator to the Alert screen capture.

Data in all columns can be sorted by clicking on the column header.



Deployment and Administration

About Program Installation

The Desktop Surveillance installation consists of several steps:

1. Installing the Desktop Surveillance Server and Administrative Panel: These components cannot be installed separately. The Desktop Surveillance Server is used to store and process all records sent by the Desktop Surveillance Clients hosted on the remote computers. The Desktop Surveillance Administrative Panel is used to manage Desktop Surveillance users and alerts and configure remote client settings.
2. Assigning Desktop Surveillance System Administrator and Supervisor: To start working with the Desktop Surveillance, you have to assign Desktop Surveillance roles to Windows users.
3. Installing Desktop Surveillance Clients: Desktop Surveillance Clients are usually installed remotely via the Desktop Surveillance Administrative Panel. A Client can be installed on any computer in the network. Desktop Surveillance Clients collect user activity data and send it to the Server.
4. Activating serial keys (adding activated serial keys): To be able to use Desktop Surveillance, you need to license it by activating purchased serial keys.
5. Assigning licenses to Desktop Surveillance Clients: Licenses are to be assigned to Desktop Surveillance Clients for the Desktop Surveillance to start receiving data from them. Clients that don't have an assigned license do not collect any user activity data, even if they are installed and launched on the computers.
6. Installing Desktop Surveillance Viewer: The Desktop Surveillance Viewer is used to review user activity records stored on the Desktop Surveillance Server. The Viewer can be installed on any computer in the network. A connection with the Desktop Surveillance Server is required for the Desktop Surveillance Viewer to operate.

After installing all Desktop Surveillance components and assigning roles and licenses, Desktop Surveillance is considered deployed and all its features become available.

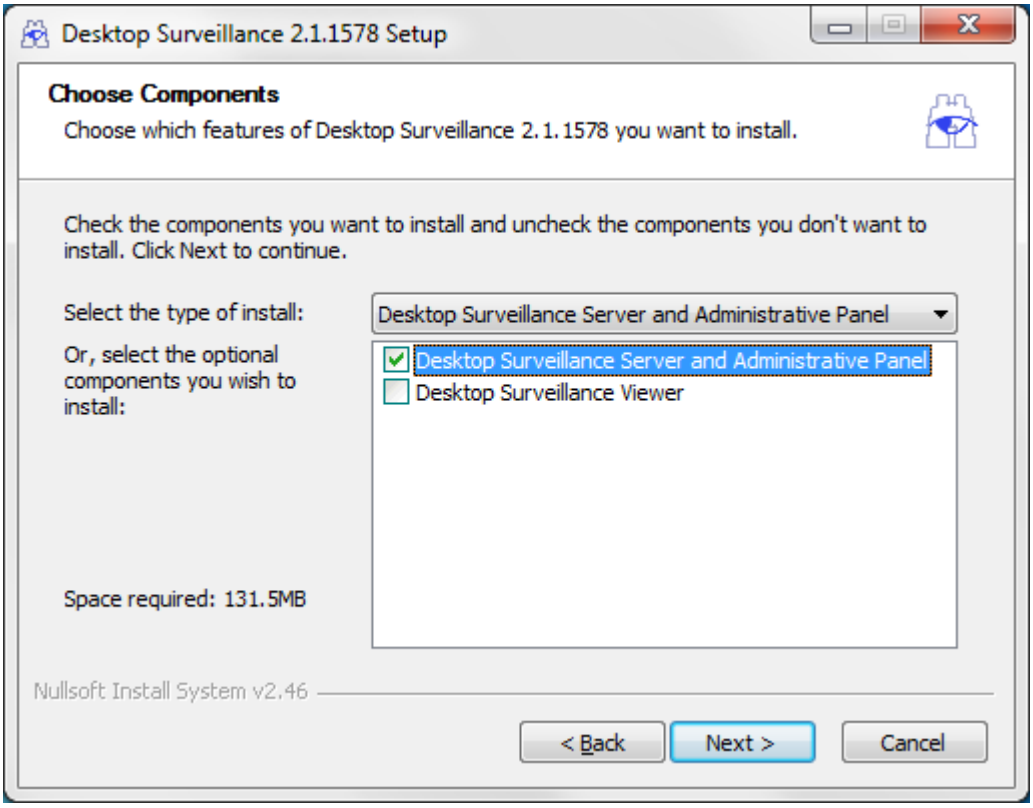
Installing/uninstalling/updating Desktop Surveillance Server

Installing Desktop Surveillance Server and Administrative Panel

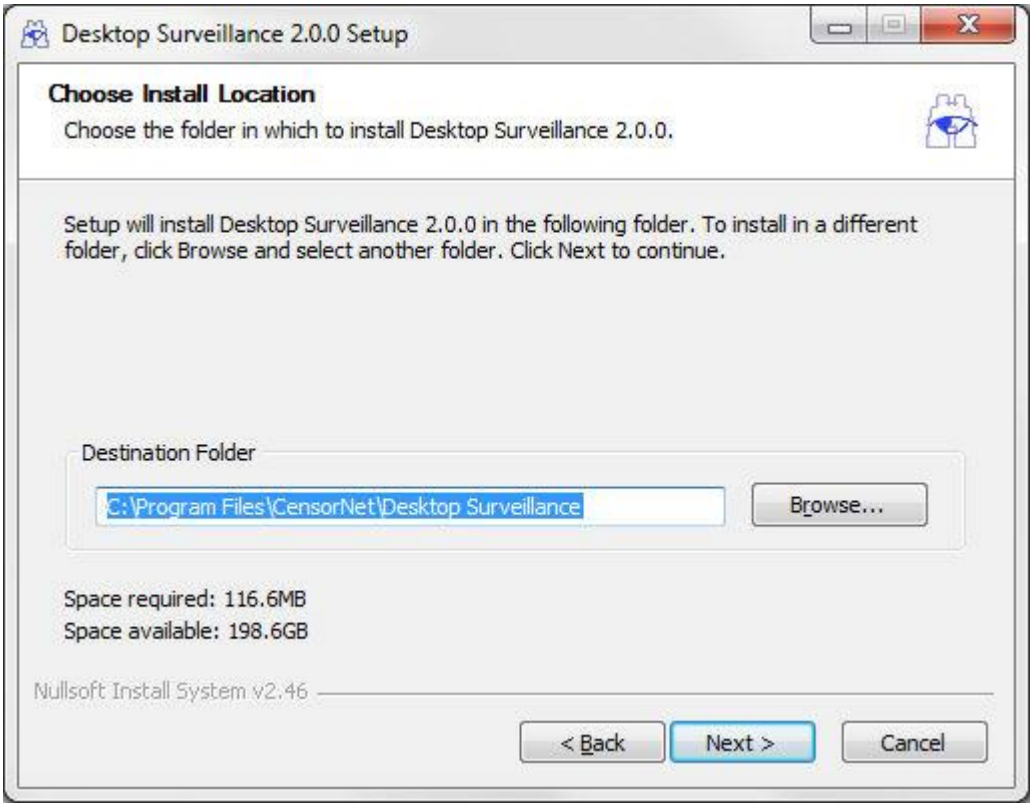
To install the CensorNet Desktop Surveillance Server and Administrative Panel, do the following:

1. Start the **CensorNet Desktop Surveillance** setup wizard.
2. Click **Next** on the **Welcome page**.
3. Carefully read the terms of the End-User Licence Agreement and click **I Agree**.
4. On the **Choose Components** page, do one of the following and click **Next**:
    - In the drop-down list, select **Server and Administrative Panel**.

- Select **Server and Administrative Panel** in the box.

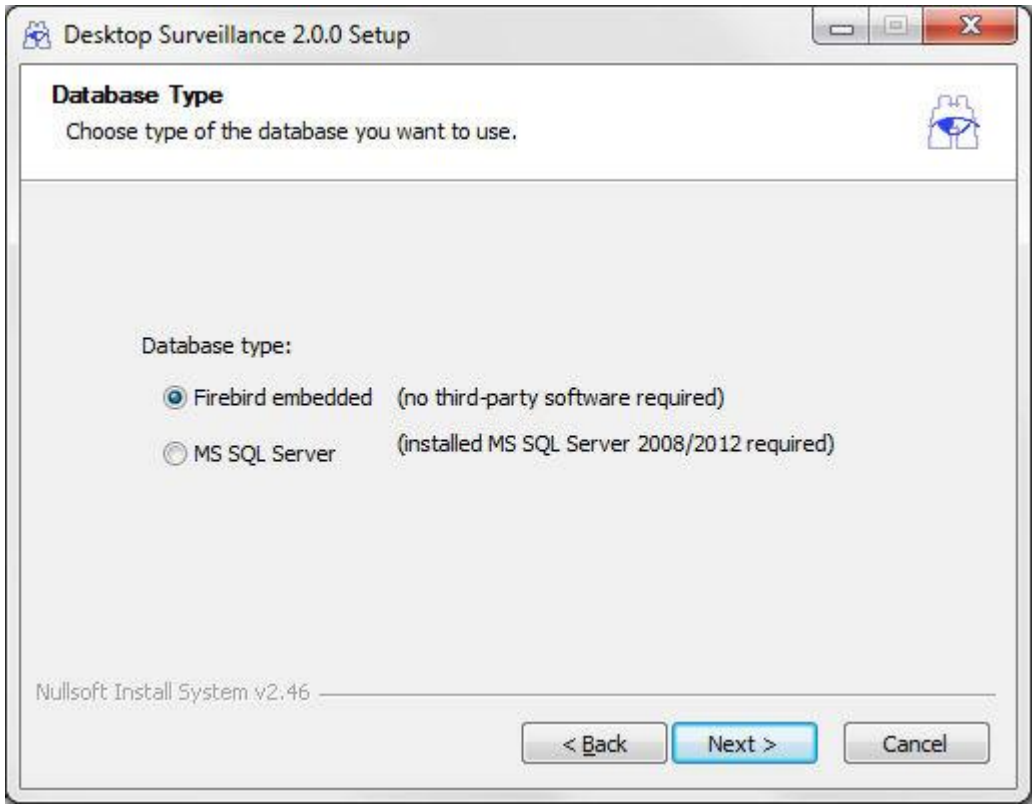

Desktop Surveillance 2.1.1578 Setup
Choose Components
Choose which features of Desktop Surveillance 2.1.1578 you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select the type of install:
Desktop Surveillance Server and Administrative Panel
Or, select the optional components you wish to install:
Desktop Surveillance Server and Administrative Panel
Desktop Surveillance Viewer
Space required: 131.5MB
Nullsoft Install System v2.46
< Back
Next >
Cancel

5. On the **Choose Install Location** page, enter the installation path or click **Browse** to navigate to the server installation folder. Click **Next.**


Desktop Surveillance 2.0.0 Setup
Choose Install Location
Choose the folder in which to install Desktop Surveillance 2.0.0.
Setup will install Desktop Surveillance 2.0.0 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.
Destination Folder
C:\Program Files\CensorNet\Desktop Surveillance
Browse...
Space required: 116.6MB
Space available: 198.6GB
Nullsoft Install System v2.46
< Back
Next >
Cancel

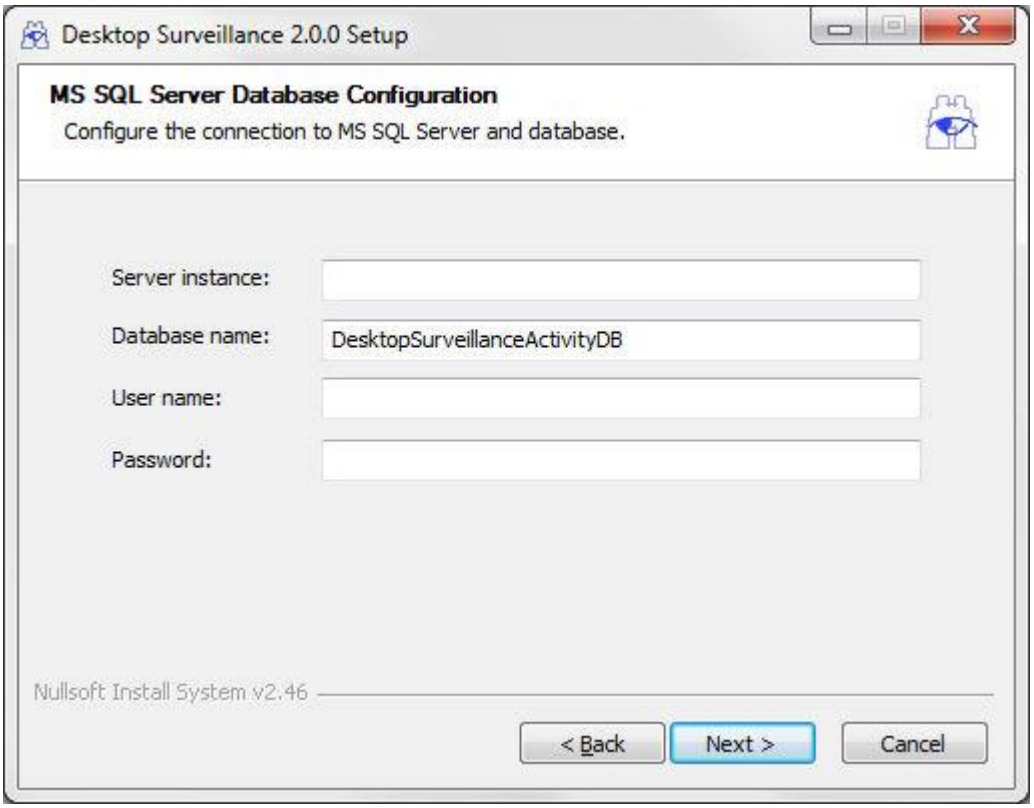
6. On the **Database Type** page, select the type of database you want to use for storing data. Click **Next**.

NOTE: If you select MS SQL Server, the screenshots will be stored in the database on MS SQL Server computer; if you select the Firebird embedded, the screenshots will be stored in Cache folder on computer on which the Server and Administrative Panel are installed.

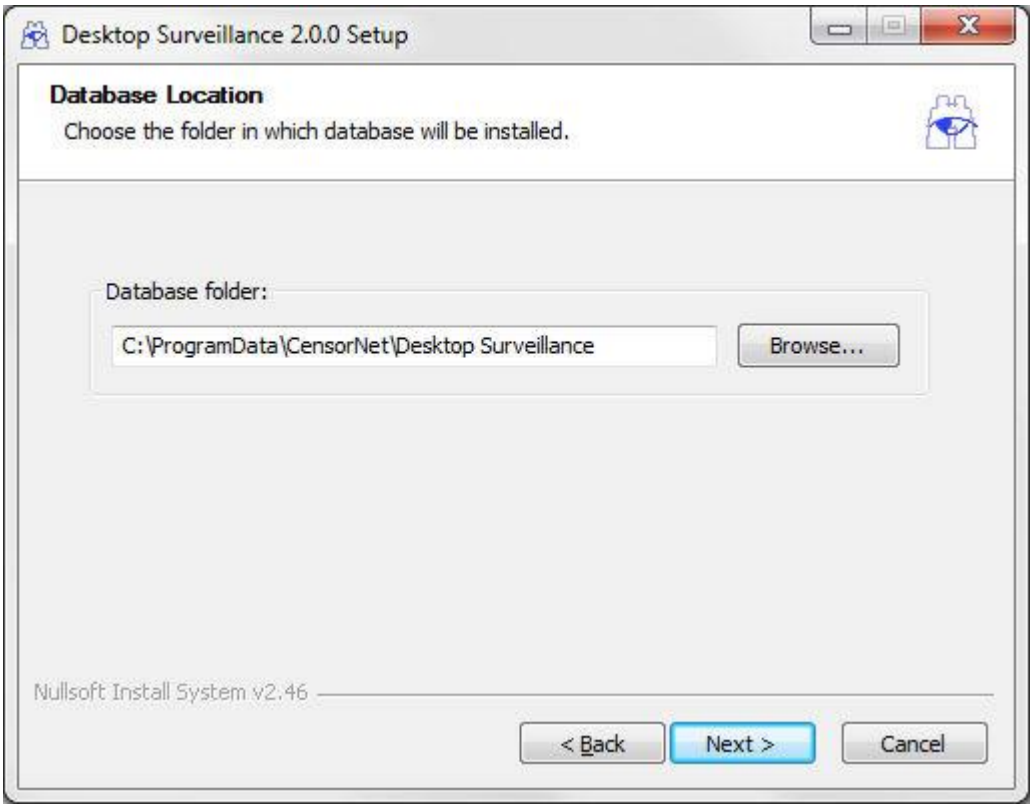


7. If you have selected **MS SQL Server**, on the **MS SQL Server Database Configuration** page, define the following connection parameters and then click **Next**:
    - Define the MS SQL **Sever instance** name defined during its installation.
    - Define the **Database name** for Desktop Surveillance database.
    - Define the **User name** and **Password** of a user account for authentication on the MS SQL Server.

      NOTE: Each time you install Server and Administrative Panel, you need to define a new database.



8. If you have selected **Firebird embedded**, on the **Database Location** page, enter the database path or click **Browse** to navigate to the database folder. Click **Next**.



9. On the **Choose Start Menu Folder** page, define the name of the folder in the start menu to which the shortcuts will be placed. Click **Install**.
10. Installation starts.

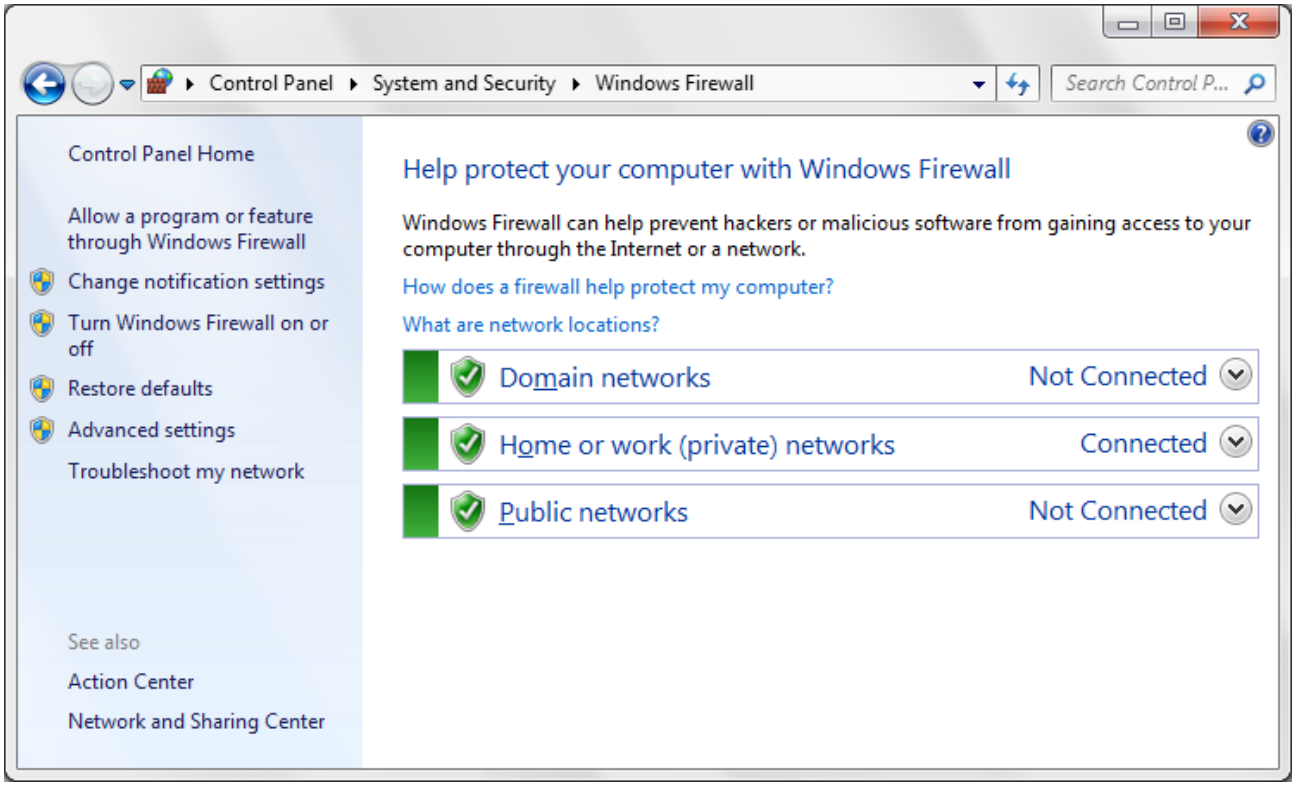
11. After the installation finishes, click **Finish**.
12. In Windows Firewall, you must allow Desktop Surveillance Server executable to accept TCP connections via ports 3346, 3347, 3349. These rules will be added to Windows Firewall automatically, if Windows Firewall is enabled during Desktop Surveillance Server installation.

NOTE: To start working with Desktop Surveillance you need the Administrator and the Supervisor accounts. It is recommended to assign roles to users immediately after installing the Server and the Administrative Panel.

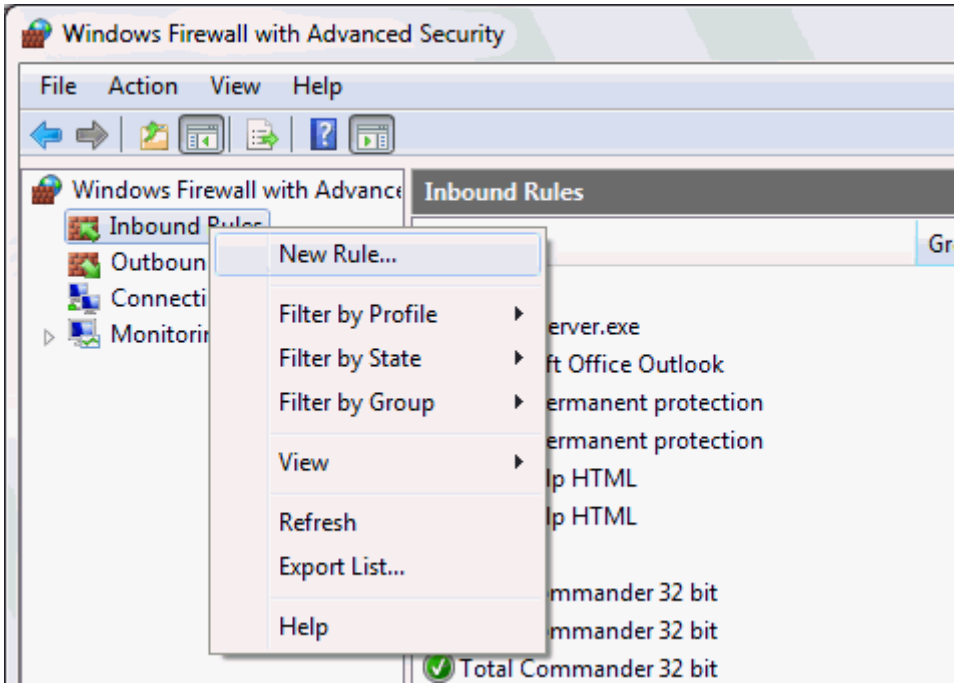
Adding Server Executable to Windows Firewall

To add Desktop Surveillance Server executable to the Windows Firewall:

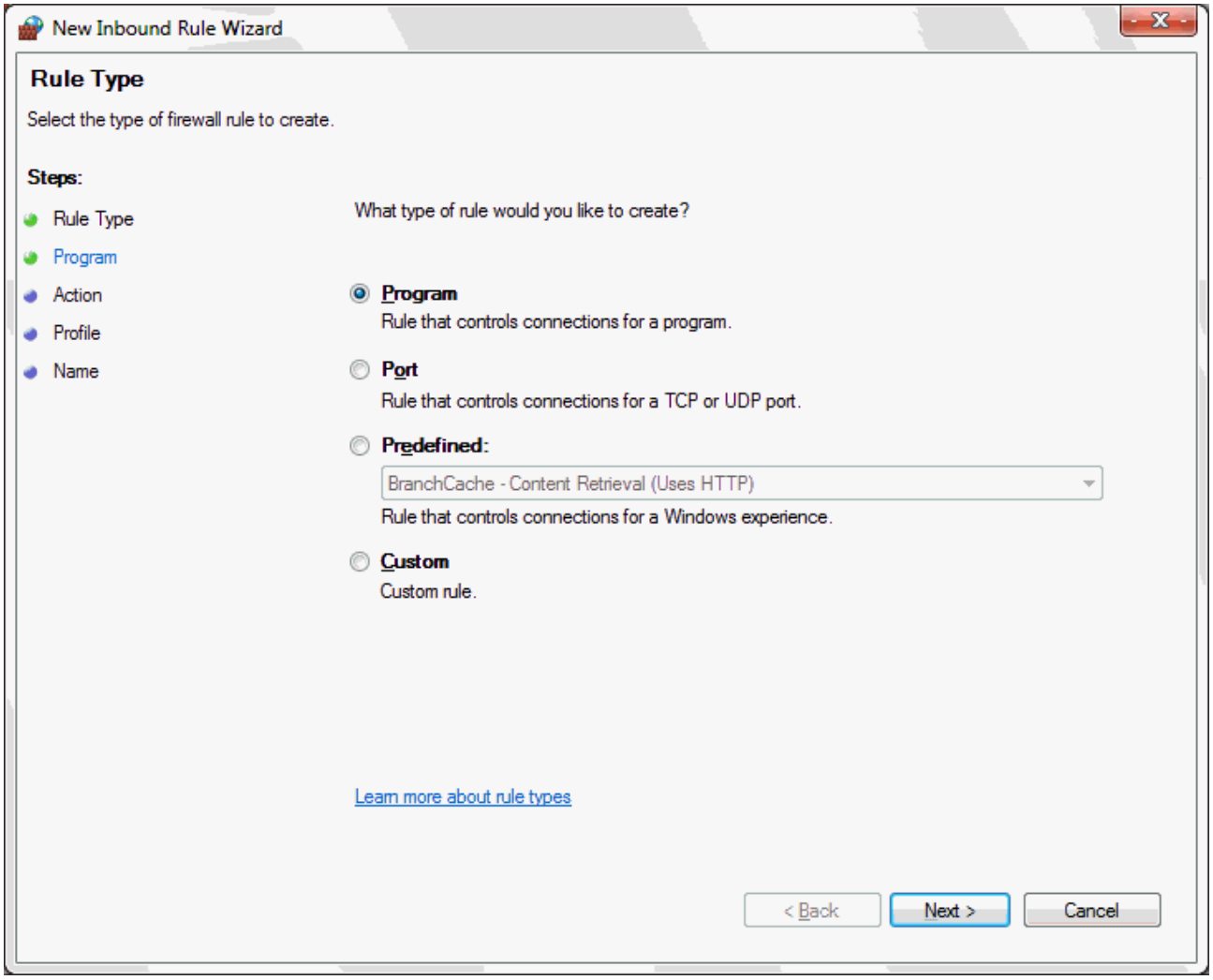
1. Select **Start > Control Panel > System and Security > Windows Firewall**.
2. The Windows Firewall window opens.


Control Panel ▸ System and Security ▸ Windows Firewall
Search Control P...
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center
Help protect your computer with Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.
How does a firewall help protect my computer?
What are network locations?
Domain networks
Not Connected
Home or work (private) networks
Connected
Public networks
Not Connected

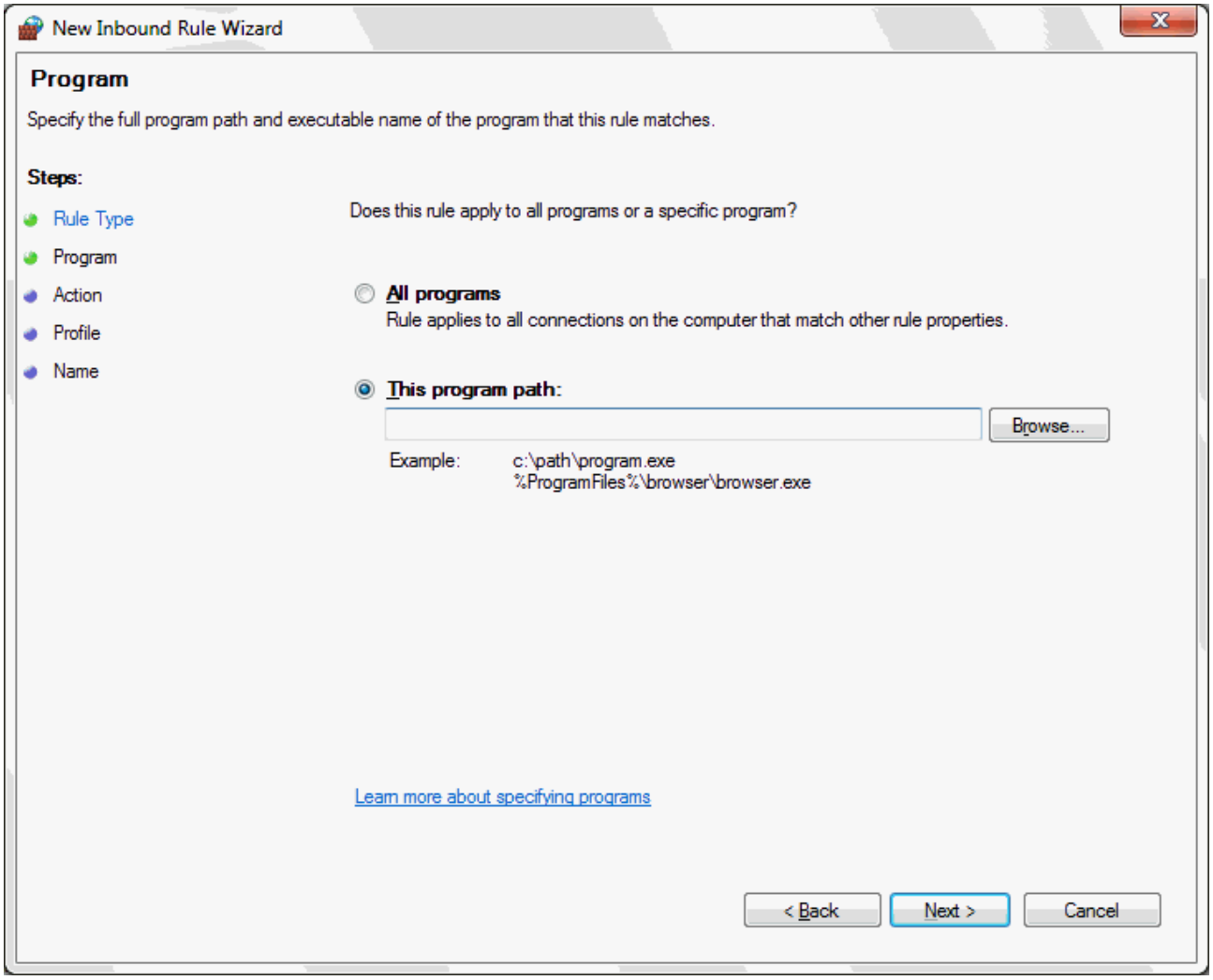
3. Click **Advanced settings**. The Windows Firewall with Advanced Security window opens.
4. Right click **Inbound Rules** and select **New rule**.



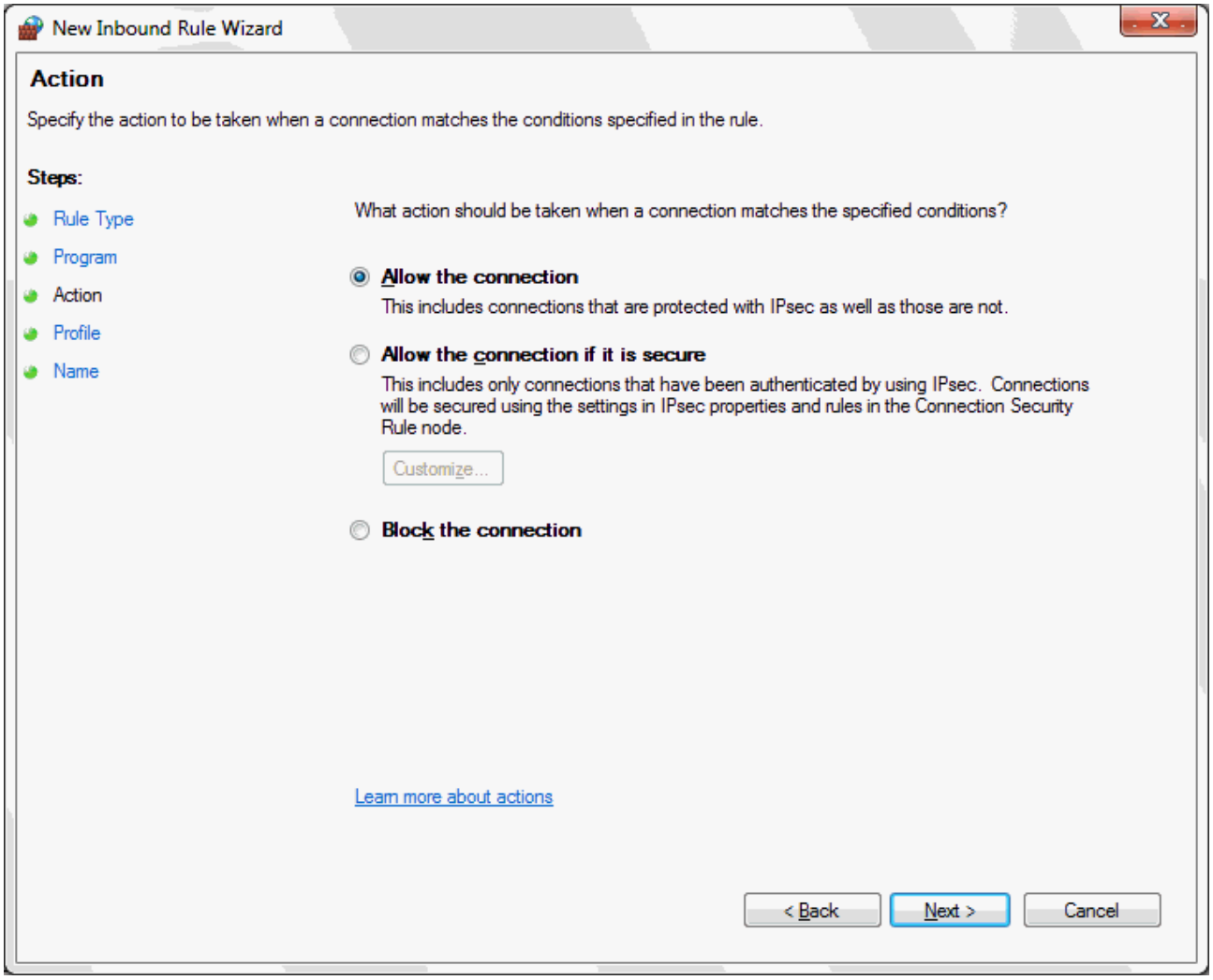
5. The New Inbound Rule Wizard opens. On the Rule Type step, select **Program** and click **Next**.



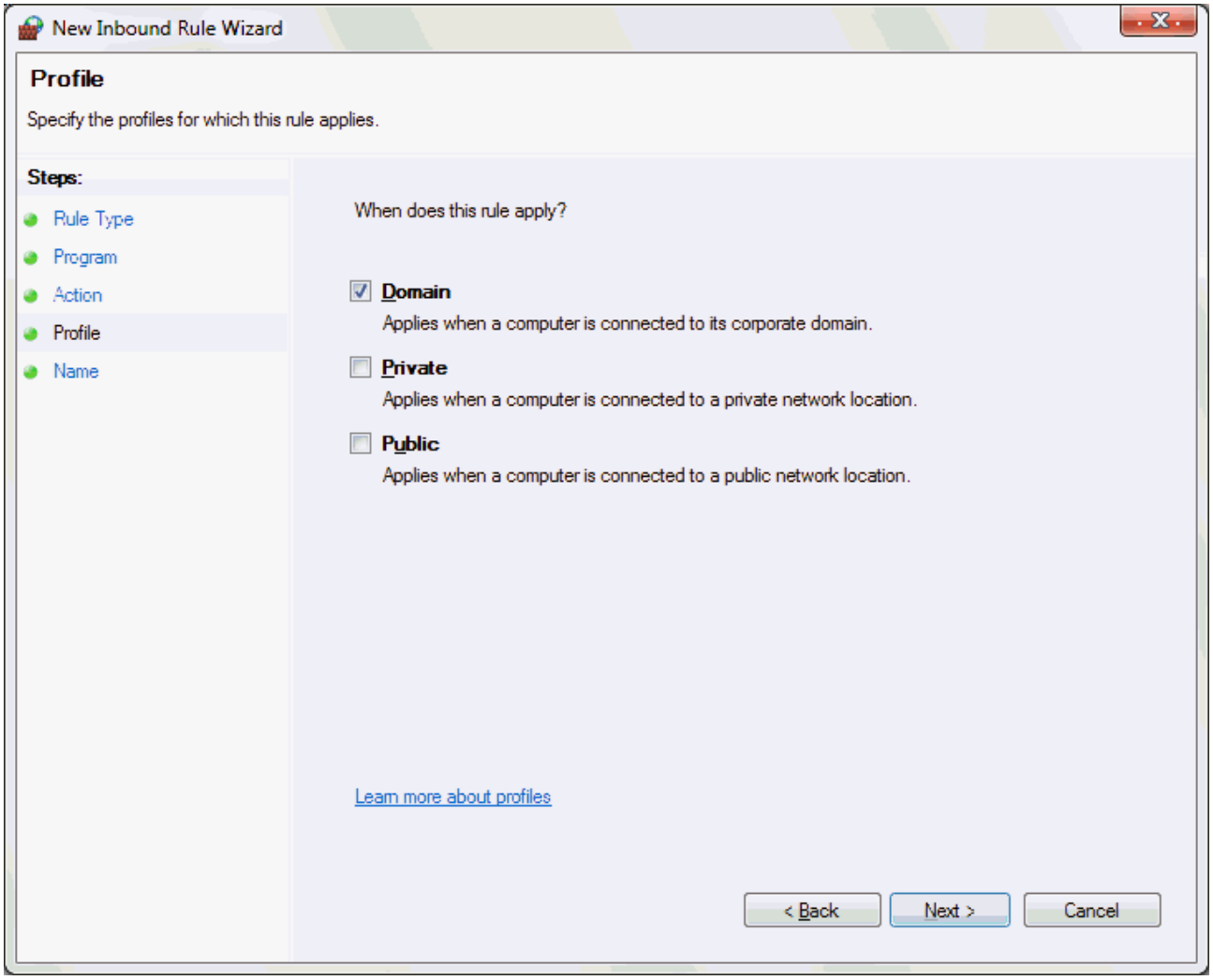
6. On the **Program** step, select **This program path**, then click **Browse** and navigate to the Desktop Surveillance Server executable. The default path is "**C:\Program Files\CensorNet\Desktop Surveillance\Server\DesktopSurveillanceServer**". Click **Next**.



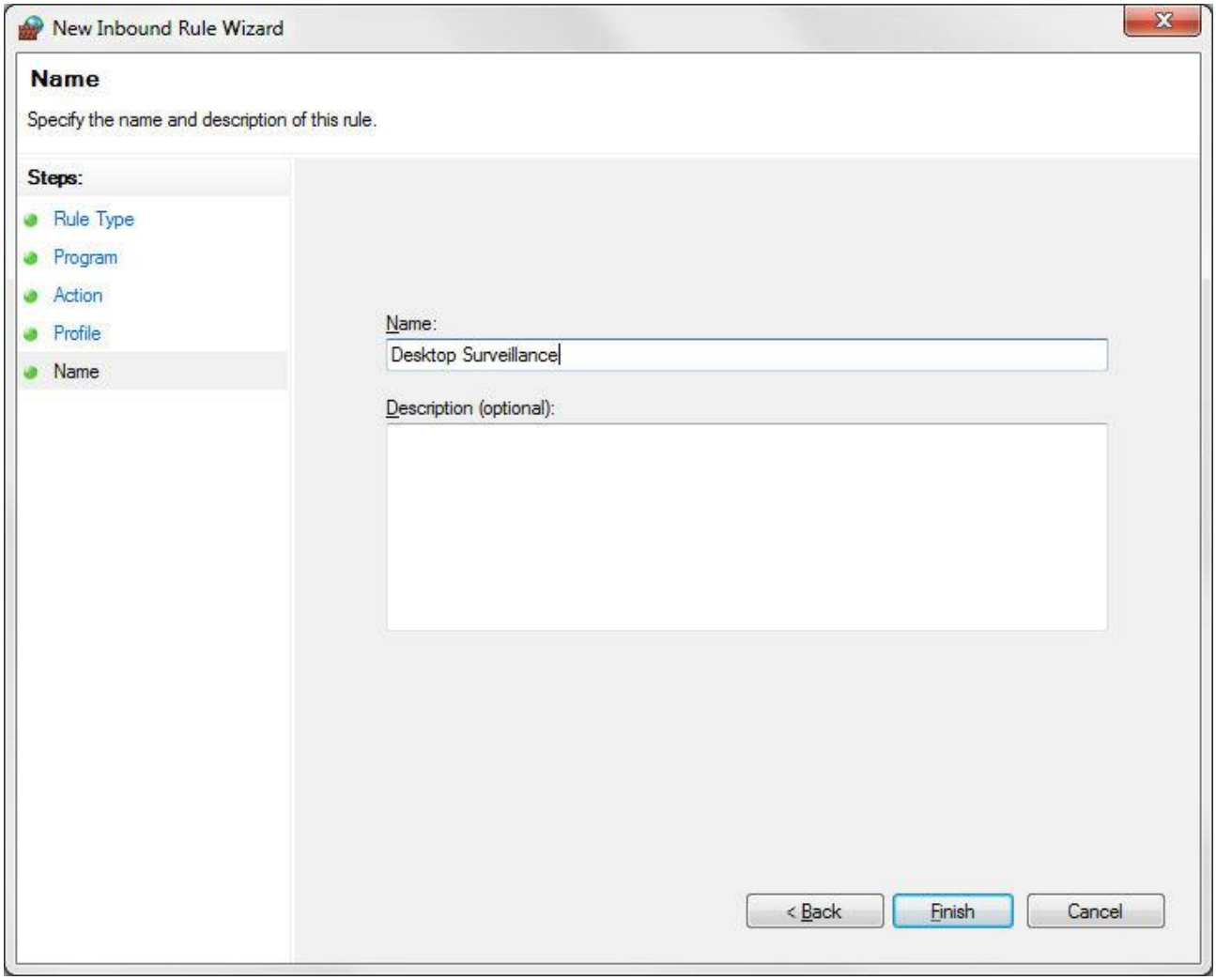
7. On the Action step, select **Allow the connection** and then click **Next**.


New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Program
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...
Block the connection
Learn more about actions
< Back
Next >
Cancel

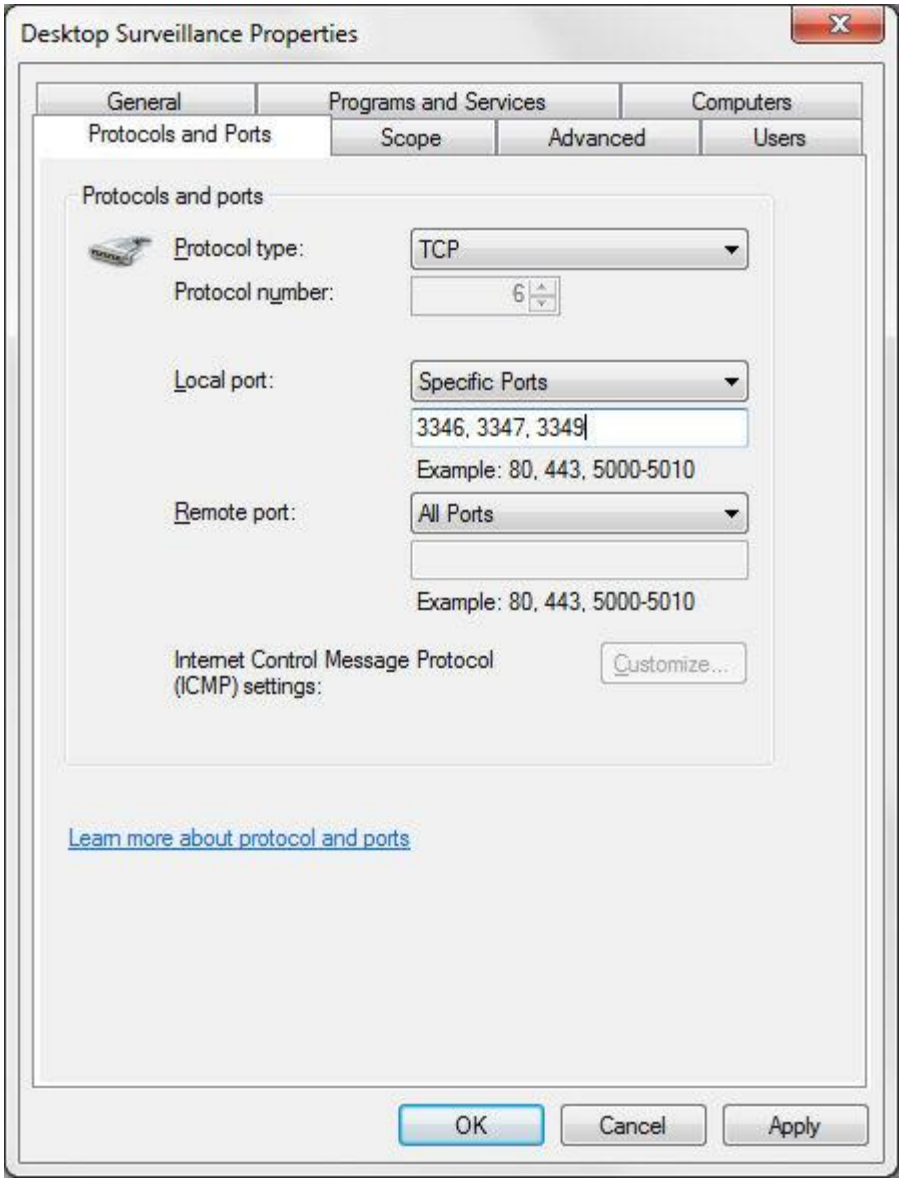
8. On the **Profile** step, select the profile of the network used for connecting remote computers and the Desktop Surveillance Server. Click **Next**.



9. On the **Name** step, define the **Name** of the rule. Click **Finish**.



10. The rule is created for the Desktop Surveillance Server application. By default, the rule allows any connections via all ports.
11. To define the protocol and ports, double click the **Desktop Surveillance** (the name you defined in the previous step) rule in the list in the Windows Firewall with Advanced Security window. The Desktop Surveillance Properties window opens.



12. In the **Protocols and Ports** tab, do the following:
    - In the **Protocol Type** list, select **TCP**.
    - In the **Local port** list, select **Specific Ports**. Type the port numbers (3346, 3347, 3349) in the box below.

    NOTE: These rules will be added to Windows Firewall automatically, if Windows Firewall is enabled during Desktop Surveillance Server installation. If you use any other Firewall, these ports and executable must be added to it as well.
13. Click **Apply** to save changes. Click **OK** to close the window.
14. Close the Windows Firewall window.

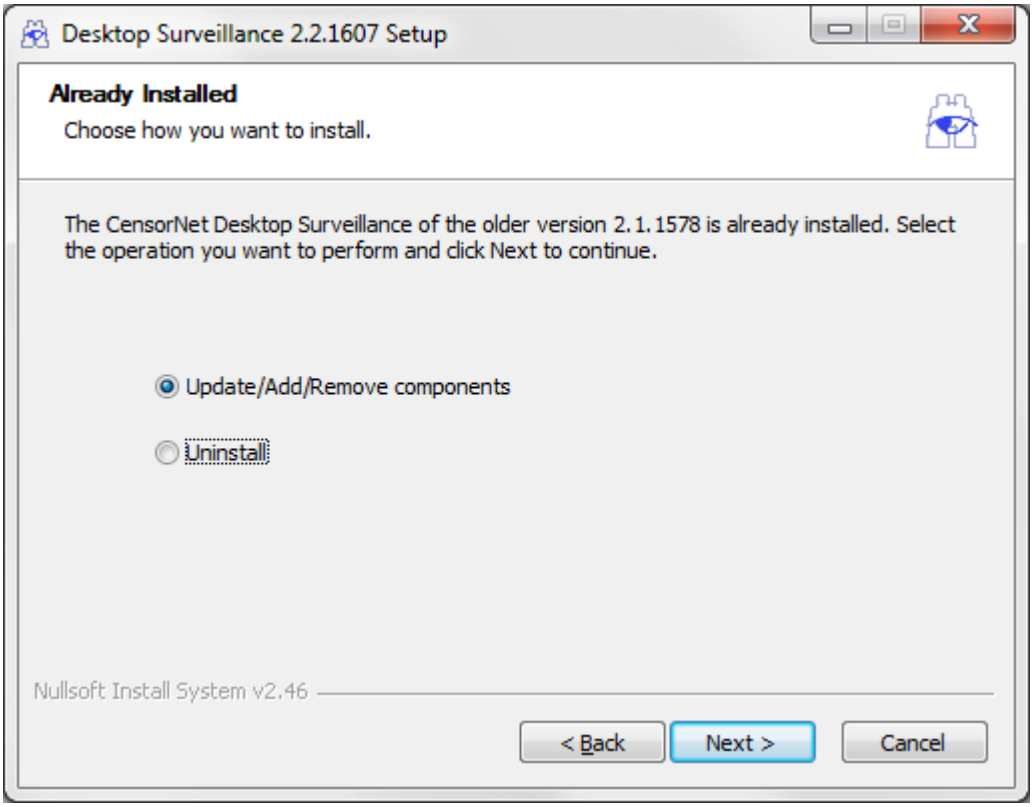
    NOTE: Unique static external IP addresses should be used for cloud-based servers.

Updating Desktop Surveillance Server

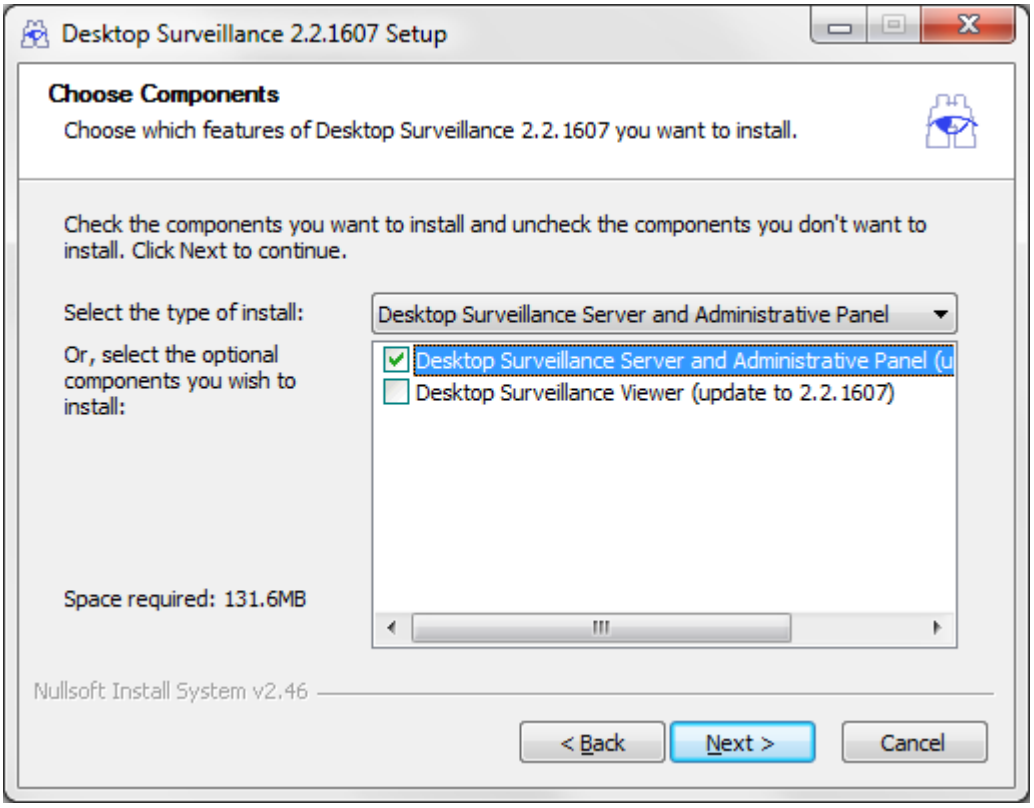
The updating of the Desktop Surveillance Server is performed via the Desktop Surveillance installation file of a newer version. During an update you may select to update the existing database to a newer version or simply reinstall it.

To update the Desktop Surveillance Server, do the following:

1. Start the **Desktop Surveillance** setup wizard.
2. On the **Welcome page**, click **Next**.
3. On the **Already Installed** page, select **Update/Add/Remove components** and click **Next**.

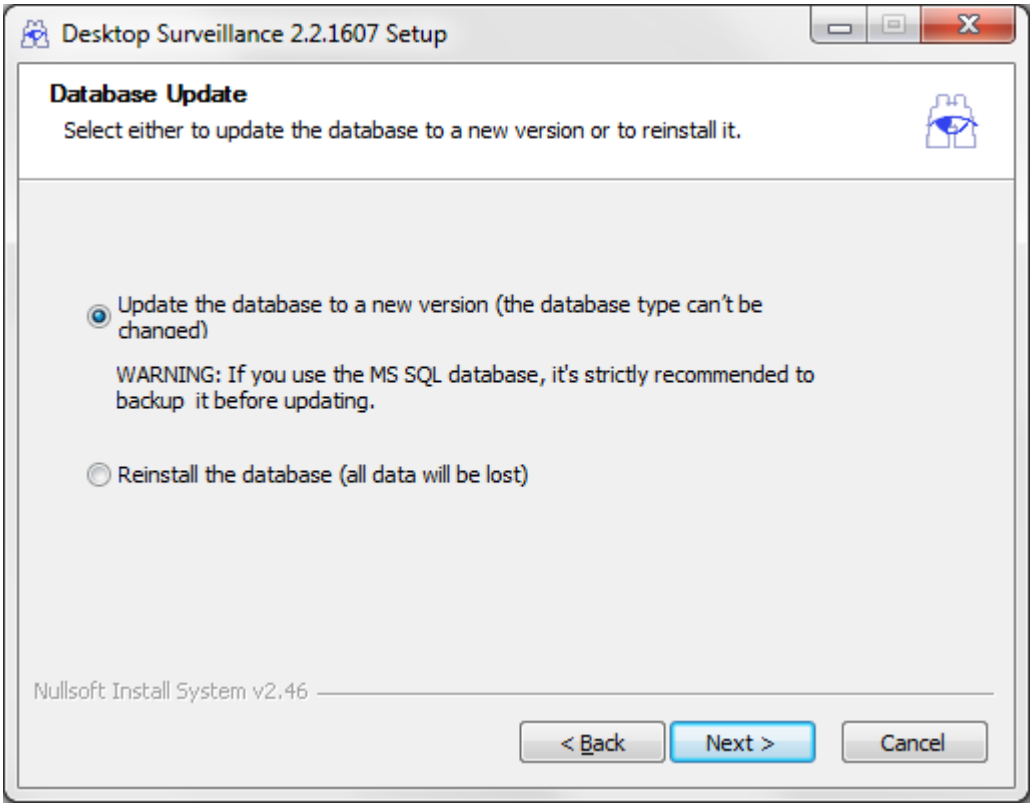

Desktop Surveillance 2.2.1607 Setup
Already Installed
Choose how you want to install.
The CensorNet Desktop Surveillance of the older version 2.1.1578 is already installed. Select the operation you want to perform and click Next to continue.
Update/Add/Remove components
Uninstall
Nullsoft Install System v2.46
< Back
Next >
Cancel

4. On the **Choose Components** page, select **Desktop Surveillance Server & Administrative Panel** and click **Next**.


Desktop Surveillance 2.2.1607 Setup
Choose Components
Choose which features of Desktop Surveillance 2.2.1607 you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select the type of install:
Desktop Surveillance Server and Administrative Panel
Or, select the optional components you wish to install:
Desktop Surveillance Server and Administrative Panel (u
Desktop Surveillance Viewer (update to 2.2.1607)
Space required: 131.6MB
Nullsoft Install System v2.46
< Back
Next >
Cancel

NOTE: If you have Desktop Surveillance Viewer installed on the same computer, you will need to select to update it as well, otherwise it will be removed.

5. On the **Database Update** page, if you want to keep the existing database, select **Update database to a new version**, otherwise select **Reinstall the database**. Click **Next**.


Desktop Surveillance 2.2.1607 Setup
Database Update
Select either to update the database to a new version or to reinstall it.
Update the database to a new version (the database type can't be changed)
WARNING: If you use the MS SQL database, it's strictly recommended to backup it before updating.
Reinstall the database (all data will be lost)
Nullsoft Install System v2.46
< Back
Next >
Cancel

NOTE: To change the type of a database, you need to reinstall the Desktop Surveillance.

6. The update process starts.
7. If the update process finishes successfully, you will see the last page of the wizard. Click **Finish** to exit the wizard.

Database Types Comparison

When installing Desktop Surveillance Server and Administrative Panel, you can choose between the two types of databases (MS SQL database and Firebird database). These databases have the following differences:

Feature	MS SQL Database	Firebird Database
Free	No (has a limited free version)	Yes
Processing speed	High	Low
Remote access to database	Yes	No
Requires additional software installation	Yes	No
Security	High	Low

Screenshots storage	Database on MS SQL Server computer	<Desktop Surveillance installation folder>/Server/Cache

Uninstalling Desktop Surveillance Server and Administrative Panel

Uninstalling Desktop Surveillance Server causes installed Desktop Surveillance Administrative Panel to be removed from the current computer as well. The Desktop Surveillance database containing all the user activity records is removed too. This operation is irreversible.

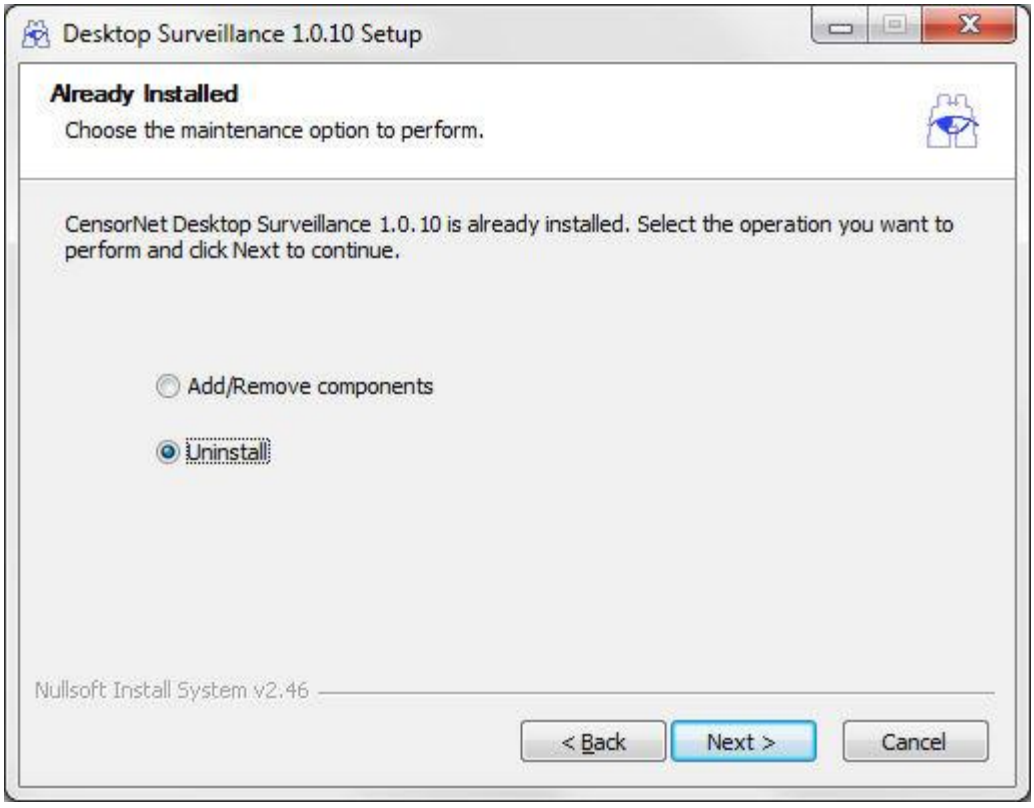
Warning! During Desktop Surveillance Server uninstallation, the database is removed without any user confirmations.

NOTE: If you reinstall the Server and there are serial keys activated online, you need to have an active Internet connection after the Server is reinstalled to synchronize the activated serial keys. If you have added activated serial keys, after the Server is reinstalled, you need to add them again.

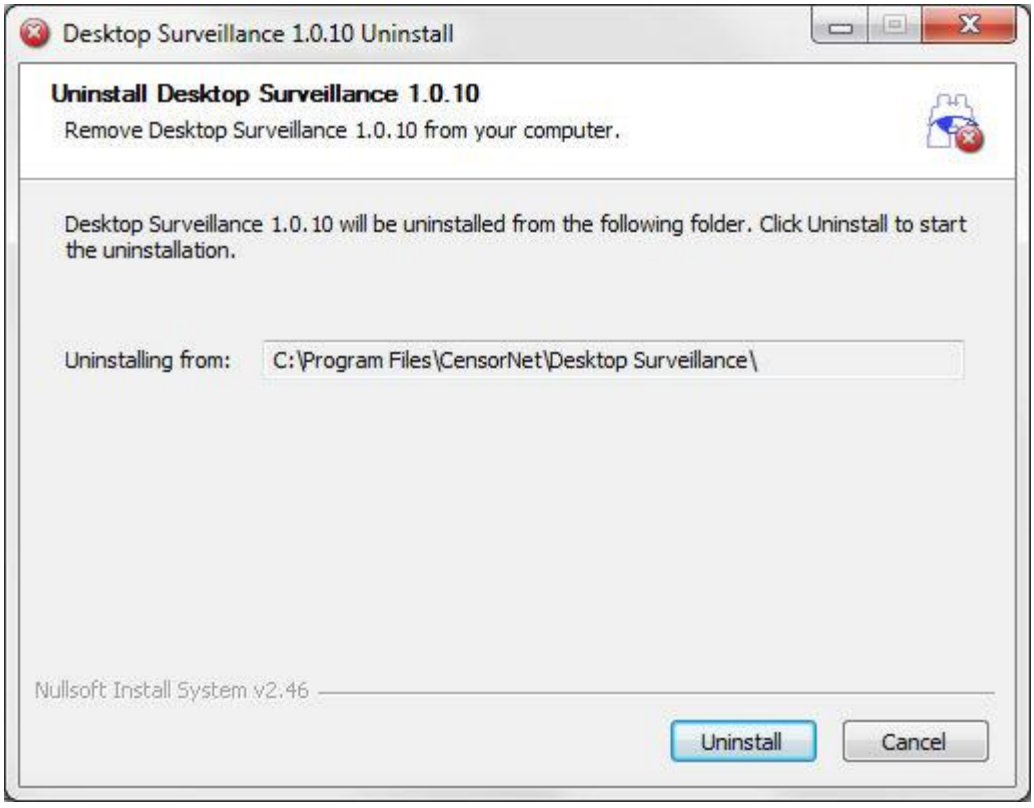
To uninstall the Desktop Surveillance Server and Administrative Panel from the local computer:

NOTE: Before uninstalling the Desktop Surveillance Server, make sure you have removed all Desktop Surveillance Clients from the remote computers. If you don't remove the Clients, they will remain installed on the remote computers and it will be impossible to remove them in a common way.

1. Start the Desktop Surveillance setup wizard by launching the setup executable (e.g. **DesktopSurveillance-1.0.10.exe**) or clicking **Uninstall/Change** on the Desktop Surveillance application in the Programs and Features window of the Windows Control Panel.
2. The setup wizard opens.
3. Click **Next** on the Welcome page.
4. The **Already Installed** page opens. Select Uninstall and click **Next**.


Desktop Surveillance 1.0.10 Setup
Already Installed
Choose the maintenance option to perform.
CensorNet Desktop Surveillance 1.0.10 is already installed. Select the operation you want to perform and click Next to continue.
Add/Remove components
Uninstall
Nullsoft Install System v2.46
< Back
Next >
Cancel

5. The Uninstall Desktop Surveillance page opens. Click **Uninstall**.


Desktop Surveillance 1.0.10 Uninstall
Uninstall Desktop Surveillance 1.0.10
Remove Desktop Surveillance 1.0.10 from your computer.
Desktop Surveillance 1.0.10 will be uninstalled from the following folder. Click Uninstall to start the uninstallation.
Uninstalling from:
C:\Program Files\CensorNet\Desktop Surveillance\
Nullsoft Install System v2.46
Uninstall
Cancel

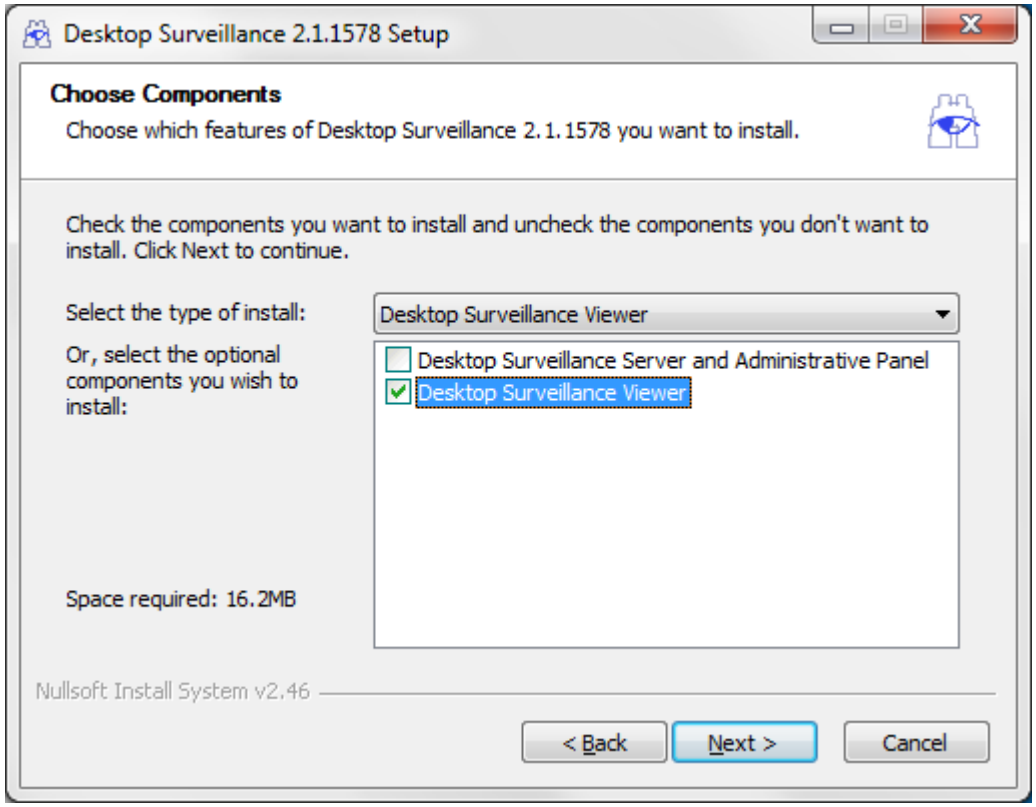
6. After the uninstallation finishes, click **Finish**.

Installing/uninstalling/updating Desktop Surveillance Viewer

Installing CensorNet Desktop Surveillance Viewer

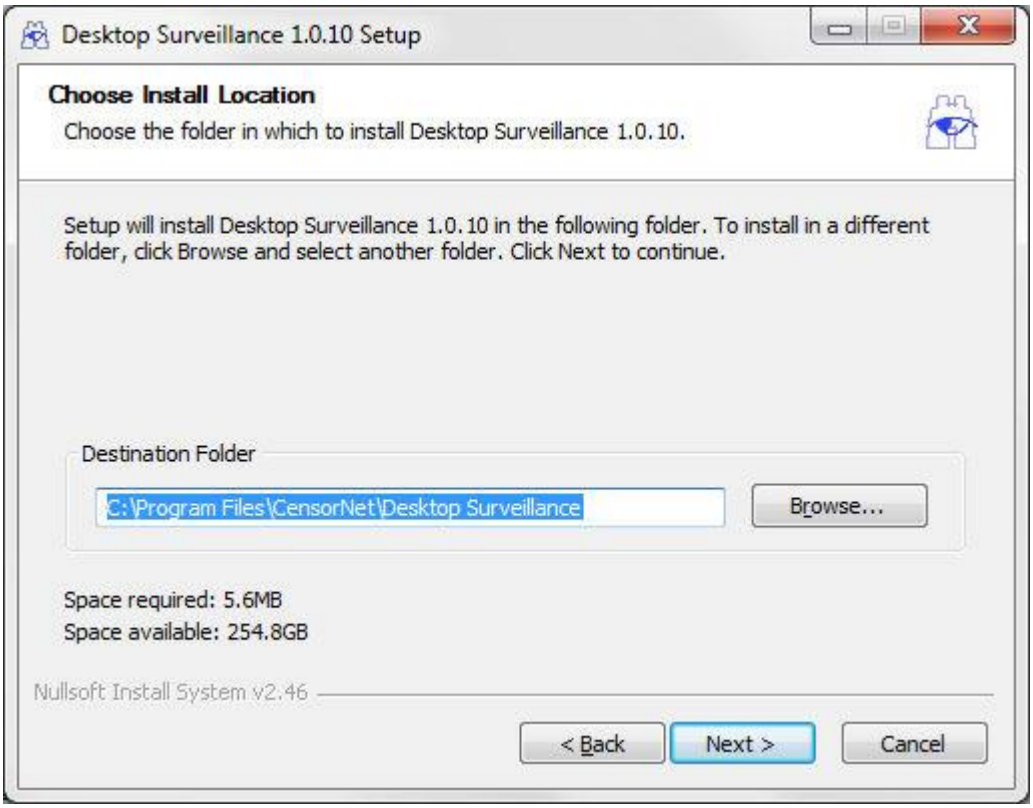
To install the CensorNet Desktop Surveillance Viewer, do the following:

1. Start the **CensorNet Desktop Surveillance** installation application.
2. On the **Welcome page**, click **Next**.
3. Carefully read the **License Agreement** and click **I Agree**.
4. On the **Choose Components** page, do one of the following and click **Next**:
    - In the drop-down list, select **Viewer**.
    - Select **Viewer** in the box.


Desktop Surveillance 2.1.1578 Setup
Choose Components
Choose which features of Desktop Surveillance 2.1.1578 you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select the type of install:
Desktop Surveillance Viewer
Or, select the optional components you wish to install:
Desktop Surveillance Server and Administrative Panel
Desktop Surveillance Viewer
Space required: 16.2MB
Nullsoft Install System v2.46
< Back
Next >
Cancel

NOTE: If you have any other Desktop Surveillance components installed on this computer, the setup wizard will offer to add or remove components and the installation procedure will differ a bit.

5. Do one of the following to define the destination folder and click **Next**:
    - Click **Browse** and in the **Browse For Folder** window, define the destination folder.
    - Enter the destination folder in the corresponding field.


Desktop Surveillance 1.0.10 Setup
Choose Install Location
Choose the folder in which to install Desktop Surveillance 1.0.10.
Setup will install Desktop Surveillance 1.0.10 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.
Destination Folder
C:\Program Files\CensorNet\Desktop Surveillance
Browse...
Space required: 5.6MB
Space available: 254.8GB
Nullsoft Install System v2.46
< Back
Next >
Cancel

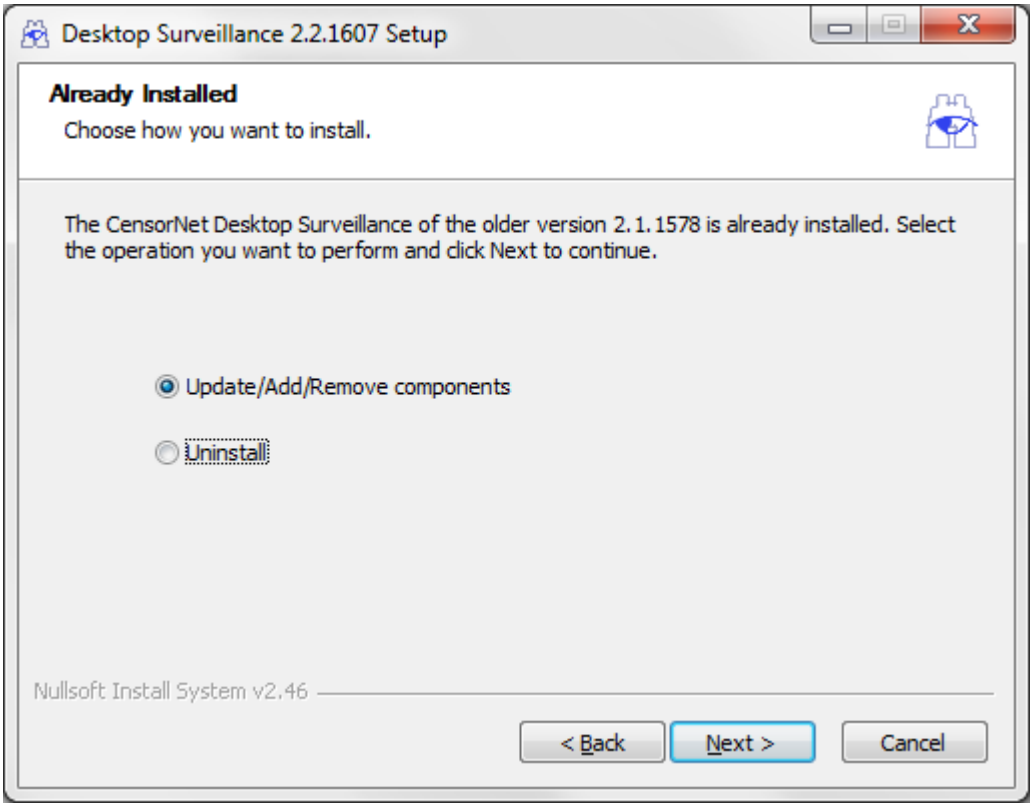
6. On the **Choose Start Menu Folder** page, do one of the following and click **Install**:
    - Define the name for the program folder in the Start Menu.
    - Select **Do not create shortcuts** to not create the program shortcuts.
7. The process of installation starts. Its progress is displayed on the **Installing** page.
8. If the installation finishes successfully, you will see the last page of the wizard. Click **Finish** to exit the wizard.

Updating the Desktop Surveillance Viewer

The updating of the Desktop Surveillance Viewer is performed via the Desktop Surveillance installation file of a newer version.

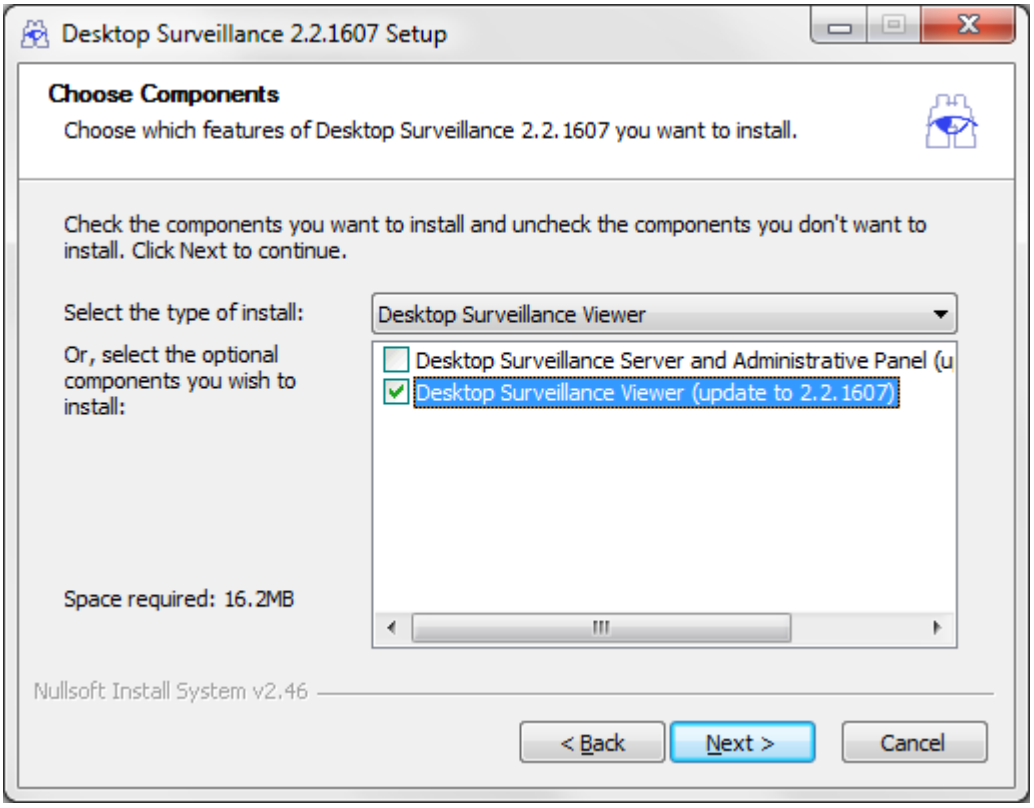
To update the Desktop Surveillance Viewer, do the following:

1. Start the Desktop Surveillance setup wizard.
2. On the **Welcome page**, click **Next**.
3. On the **Already Installed** page, select **Update/Add/Remove components** and click **Next**.


Desktop Surveillance 2.2.1607 Setup
Already Installed
Choose how you want to install.
The CensorNet Desktop Surveillance of the older version 2.1.1578 is already installed. Select the operation you want to perform and click Next to continue.
Update/Add/Remove components
Uninstall
Nullsoft Install System v2.46
< Back
Next >
Cancel

NOTE: If you have Desktop Surveillance Server and Administrative Panel installed on the same computer, you will need to select to update them as well, otherwise they will be removed.

4. On the **Choose Components** page, select **Desktop Surveillance Viewer** and click **Next**.


Desktop Surveillance 2.2.1607 Setup
Choose Components
Choose which features of Desktop Surveillance 2.2.1607 you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select the type of install:
Desktop Surveillance Viewer
Or, select the optional components you wish to install:
Desktop Surveillance Server and Administrative Panel (u
Desktop Surveillance Viewer (update to 2.2.1607)
Space required: 16.2MB
Nullsoft Install System v2.46
< Back
Next >
Cancel

5. The update process starts.
6. If the update process finishes successfully, you will see the last page of the wizard. Click **Finish** to exit the wizard.

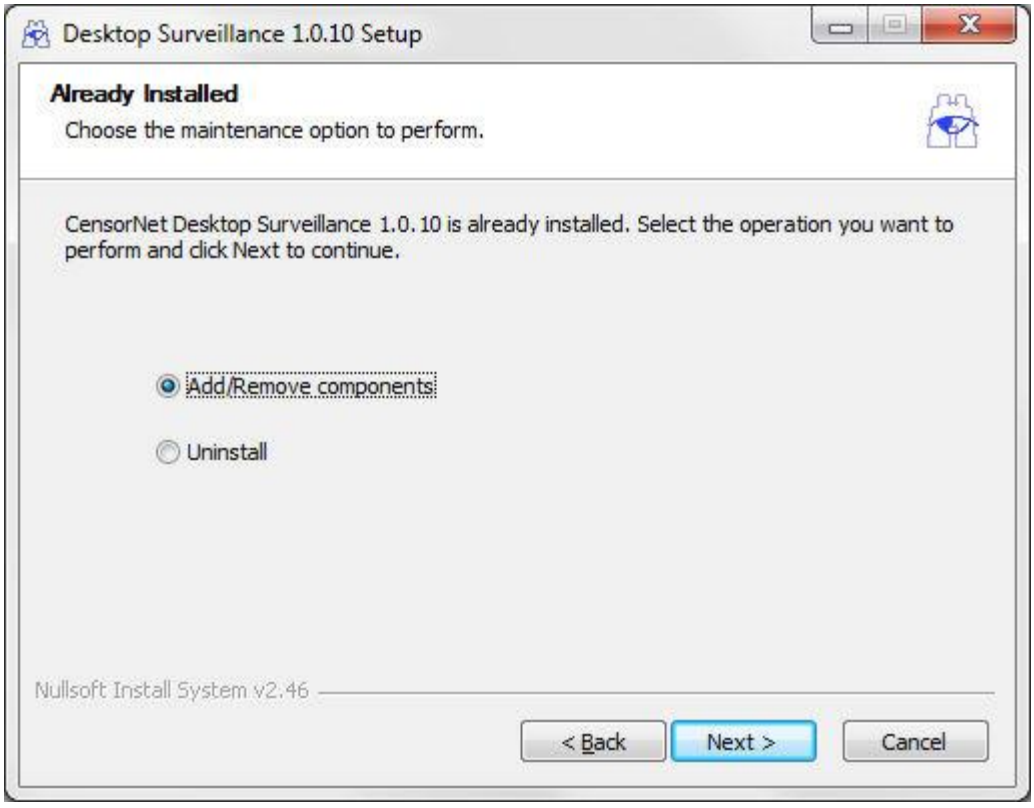
Uninstalling Desktop Surveillance Viewer

Uninstallation of the Desktop Surveillance Viewer can be performed in 2 ways:

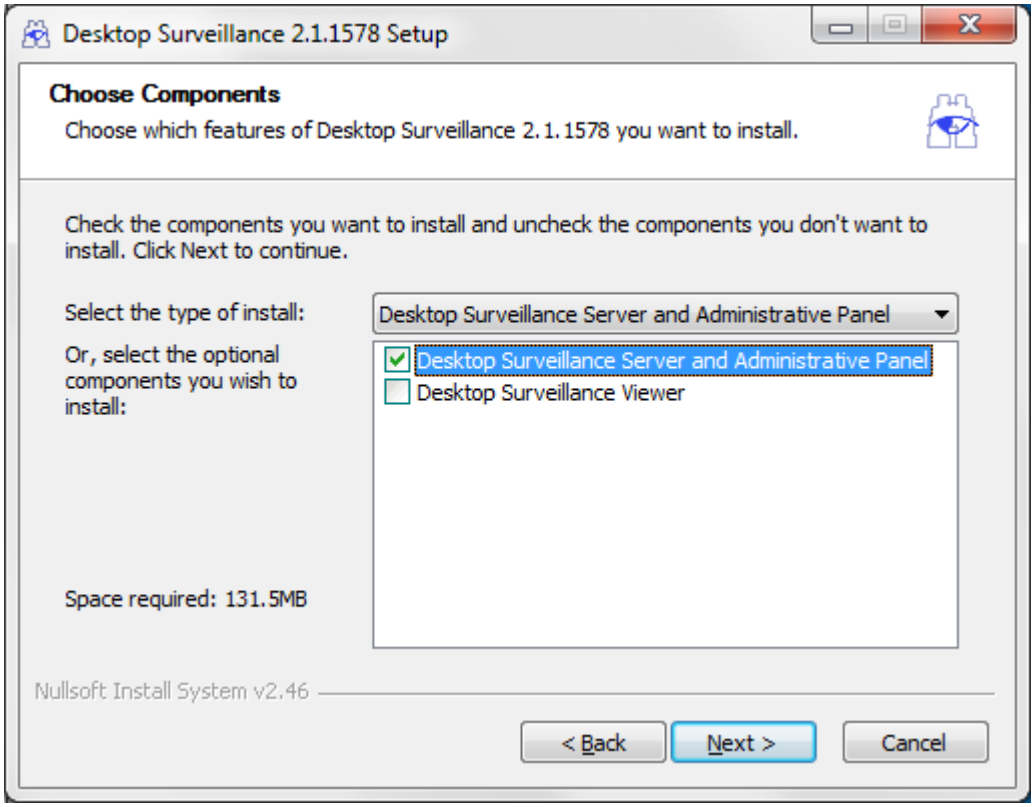
- Via the Desktop Surveillance setup wizard by choosing Add/Remove components: This method should be used when Desktop Surveillance Viewer is installed together with any other Desktop Surveillance components.
- Through Programs and Components in the Windows Control Panel: If you want to remove only **Viewer** application, use this method only when no other components are installed on the computer along with Desktop Surveillance Viewer. This method is intended to remove all Desktop Surveillance components installed on the current PC.

To uninstall the Viewer that is installed along with the Desktop Surveillance Server:

1. Run the Desktop Surveillance setup package (**DesktopSurveillance-1.0.10.exe**).
2. Click **Next** on the Welcome page.
3. On the Already Installed page, select Add/Remove components and click **Next**.


Desktop Surveillance 1.0.10 Setup
Already Installed
Choose the maintenance option to perform.
CensorNet Desktop Surveillance 1.0.10 is already installed. Select the operation you want to perform and click Next to continue.
Add/Remove components
Uninstall
Nullsoft Install System v2.46
< Back
Next >
Cancel

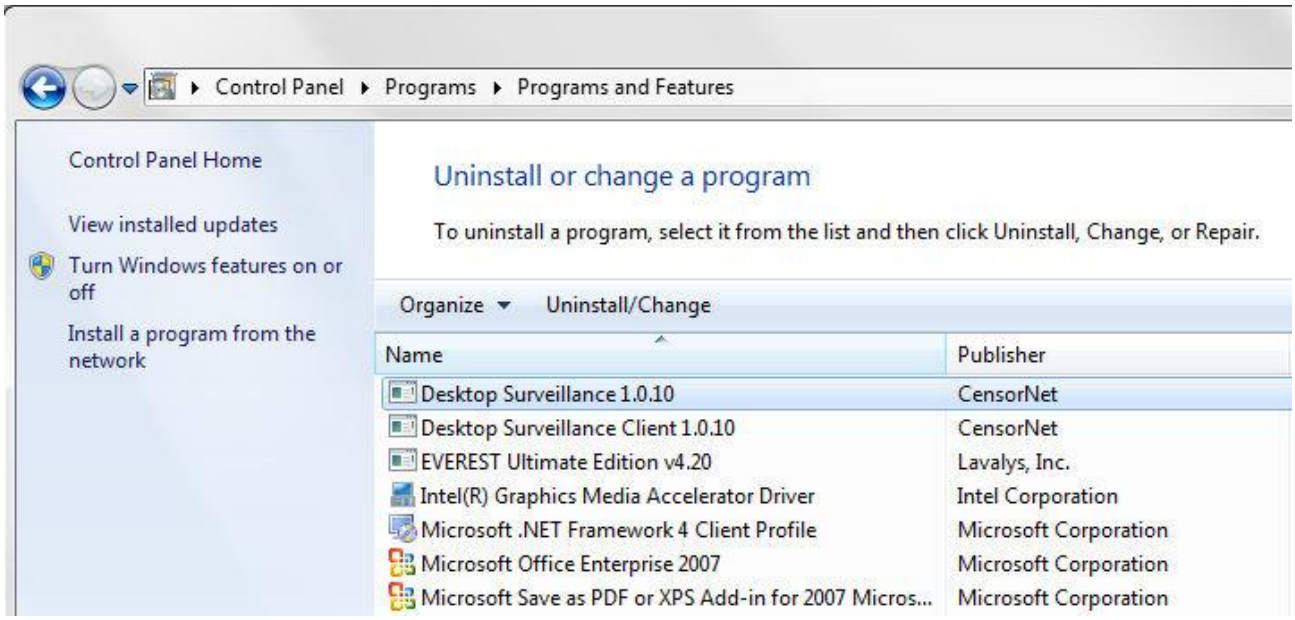
4. The Choose Components page opens. Clear the Viewer check box and click **Next**.


Desktop Surveillance 2.1.1578 Setup
Choose Components
Choose which features of Desktop Surveillance 2.1.1578 you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select the type of install:
Desktop Surveillance Server and Administrative Panel
Or, select the optional components you wish to install:
Desktop Surveillance Server and Administrative Panel
Desktop Surveillance Viewer
Space required: 131.5MB
Nullsoft Install System v2.46
< Back
Next >
Cancel

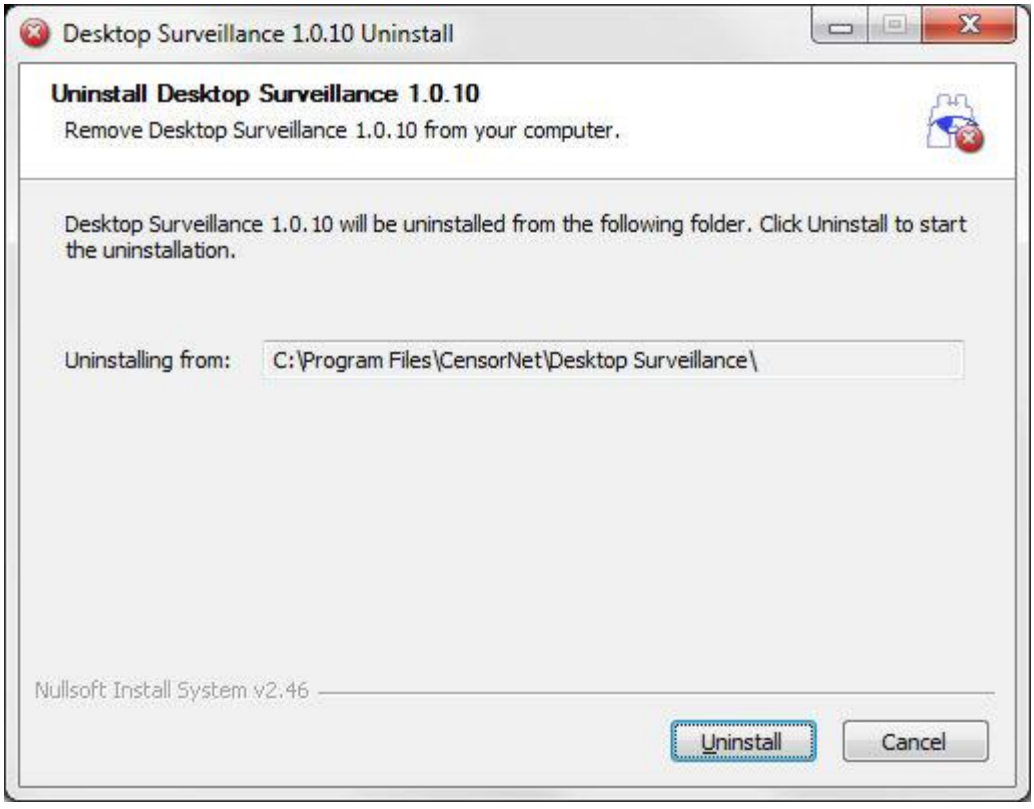
5. The setup wizard removes the unselected components.
6. When uninstallation is complete, click **Finish**.

To uninstall the Viewer that is installed alone on a separate computer:

1. Open the Windows Control Panel and navigate to the Programs and Components page.
2. Select Desktop Surveillance in the programs list and click Uninstall/Change on the toolbar.


Control Panel ▸ Programs ▸ Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network
Uninstall or change a program
To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.
Organize
Uninstall/Change
Name
Publisher
Desktop Surveillance 1.0.10
CensorNet
Desktop Surveillance Client 1.0.10
CensorNet
EVEREST Ultimate Edition v4.20
Lavalys, Inc.
Intel(R) Graphics Media Accelerator Driver
Intel Corporation
Microsoft .NET Framework 4 Client Profile
Microsoft Corporation
Microsoft Office Enterprise 2007
Microsoft Corporation
Microsoft Save as PDF or XPS Add-in for 2007 Micros...
Microsoft Corporation

3. The Uninstall Desktop Surveillance page opens. Click **Uninstall**.


Desktop Surveillance 1.0.10 Uninstall
Uninstall Desktop Surveillance 1.0.10
Remove Desktop Surveillance 1.0.10 from your computer.
Desktop Surveillance 1.0.10 will be uninstalled from the following folder. Click Uninstall to start the uninstallation.
Uninstalling from:
C:\Program Files\CensorNet\Desktop Surveillance\
Nullsoft Install System v2.46
Uninstall
Cancel

4. Wait for the setup wizard to complete uninstallation and click **Finish**.

Installing/uninstalling/updating Desktop Surveillance Clients

About Desktop Surveillance Clients Installation

During Desktop Surveillance deployment, remote installation of Desktop Surveillance Clients is used. Remote installation of Desktop Surveillance Clients is performed via Administrative Panel.

To ensure successful remote installation of Desktop Surveillance Clients, you have to set up the network environment beforehand. If your computers belong to a workgroup but not a domain, you need to know the administrator account credentials for each remote computer. Otherwise knowing the Domain Administrator credentials is enough.

Desktop Surveillance also features installing Clients (either local or remote) via the installation package generated in the Administrative Panel. Thus you can distribute the installation package of the Client with predefined settings among the network computers and install it. This kind of installation is useful when you experience difficulties with installing Desktop Surveillance Clients remotely via Administrative Panel, or the computers in your network are part of a workgroup and do not have the same administrative account for each computer.

NOTE: The Desktop Surveillance Client installed locally via setup wizard is only capable of interacting with the local Desktop Surveillance Server. For Desktop Surveillance deployment use other installation methods.

Client Installation prerequisites

Setting up Environment for Client Remote Installation

You might need to make changes to your network configuration for successful Desktop Surveillance installation, and for its components normal interaction.

The majority of Clients installation/uninstallation issues are caused by incorrect system or network settings.

The following conditions have to be met for successful Desktop Surveillance Client installation:

- The remote computer has to be online and accessible via network.
- Shared folders have to be accessible on the remote computer. Simple file sharing (Sharing Wizard) has to be disabled.
- You need to know the domain administrator or local administrator account credentials for the remote computer.
- The Server and the Remote Procedure Call (RPC) system services have to be running on the remote computer.
- Windows XP and Vista Firewall has to be disabled on the remote computer during the Clients remote installation.

- In Windows 7 and Server 2008 Firewall, allow inbound connections in the Remote Service Management (RPC) rule for the remote computers (in this case it is not necessary to disable Windows Firewall)
- In Windows Firewall on the Server side, allow Desktop Surveillance Server executable to accept TCP connections via ports 3346, 3347, 3349:

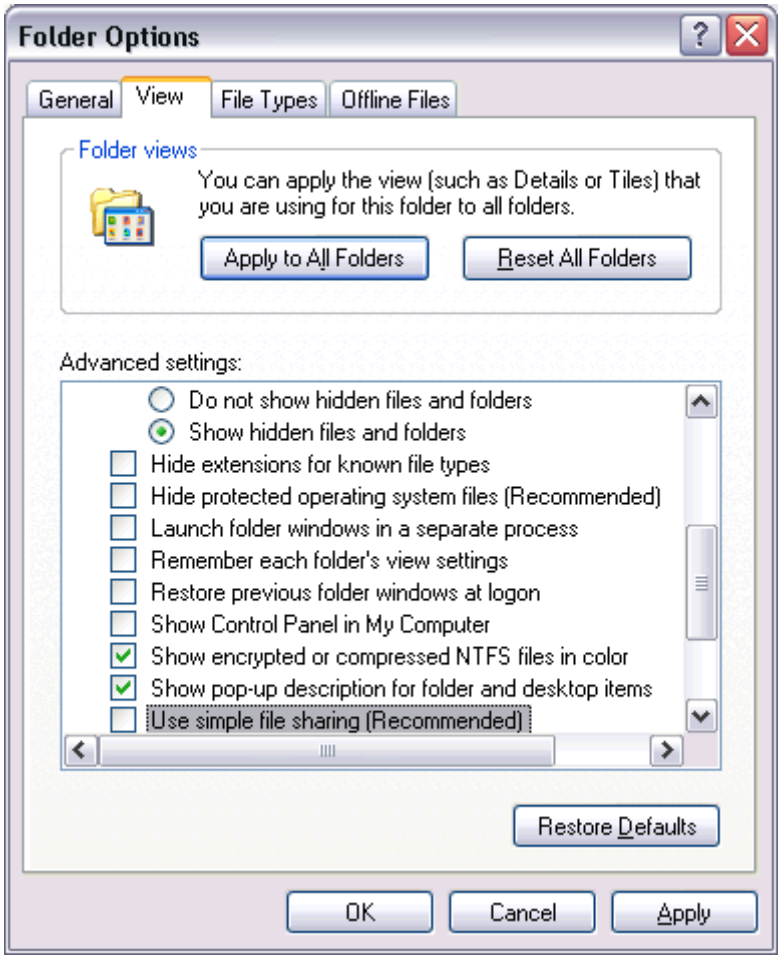
  NOTE: These rules will be added to Windows Firewall automatically, if Windows Firewall is enabled during Desktop Surveillance Server installation.

Make sure the conditions mentioned above are met to avoid possible problems with Client remote installation.

Disabling Simple File Sharing in Windows XP

To disable Simple file sharing in Windows XP, do the following:

1. Open **My Computer**.
2. Select **Tools > Folder Options** in the menu.
3. The Folder Options window opens. Select the View tab.

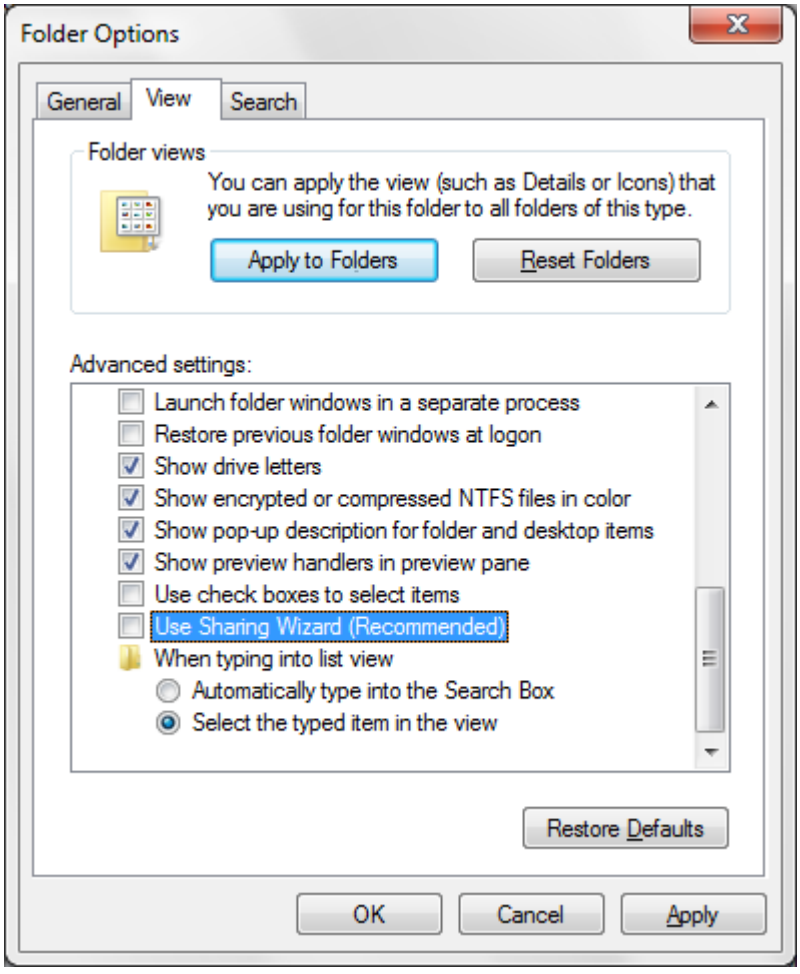

Folder Options
General
View
File Types
Offline Files
Folder views
You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.
Apply to All Folders
Reset All Folders
Advanced settings:
Do not show hidden files and folders
Show hidden files and folders
Hide extensions for known file types
Hide protected operating system files (Recommended)
Launch folder windows in a separate process
Remember each folder's view settings
Restore previous folder windows at logon
Show Control Panel in My Computer
Show encrypted or compressed NTFS files in color
Show pop-up description for folder and desktop items
Use simple file sharing (Recommended)
Restore Defaults
OK
Cancel
Apply

4. Clear the **Use simple file sharing** check box.
5. Click **Apply** and **OK** to close the window.

Disabling Sharing Wizard in Windows 7

To disable the Sharing wizard in Windows 7, do the following:

1. Open **Computer**.
2. Select **Organize > Folder and search options**.
3. The Folder Options window opens. Select the View tab.

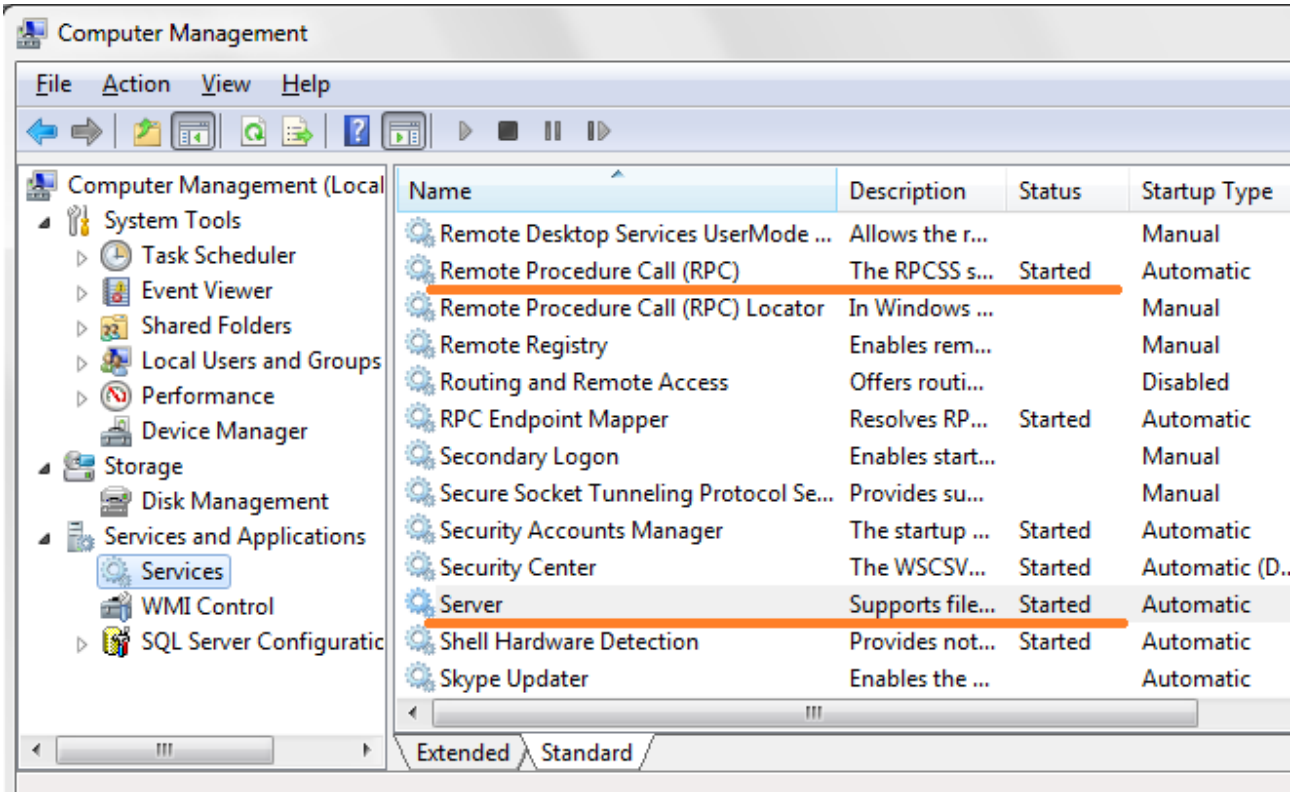

Folder Options
General
View
Search
Folder views
You can apply the view (such as Details or Icons) that you are using for this folder to all folders of this type.
Apply to Folders
Reset Folders
Advanced settings:
Launch folder windows in a separate process
Restore previous folder windows at logon
Show drive letters
Show encrypted or compressed NTFS files in color
Show pop-up description for folder and desktop items
Show preview handlers in preview pane
Use check boxes to select items
Use Sharing Wizard (Recommended)
When typing into list view
Automatically type into the Search Box
Select the typed item in the view
Restore Defaults
OK
Cancel
Apply

4. Clear the **Use Sharing Wizard** check box.
5. Click **Apply** and **OK** to close the window.

Checking System Services

To check that the Server and Remote Procedure Call (RPC) system services are running:

1. Right click **Computer** and select **Manage**. Computer Management opens.
2. Expand the Services and Applications node and select Services.
3. Find the Server service and the Remote Procedure Call (RPC) service in the list of services. Make sure both services are running (they status is displayed as Started).



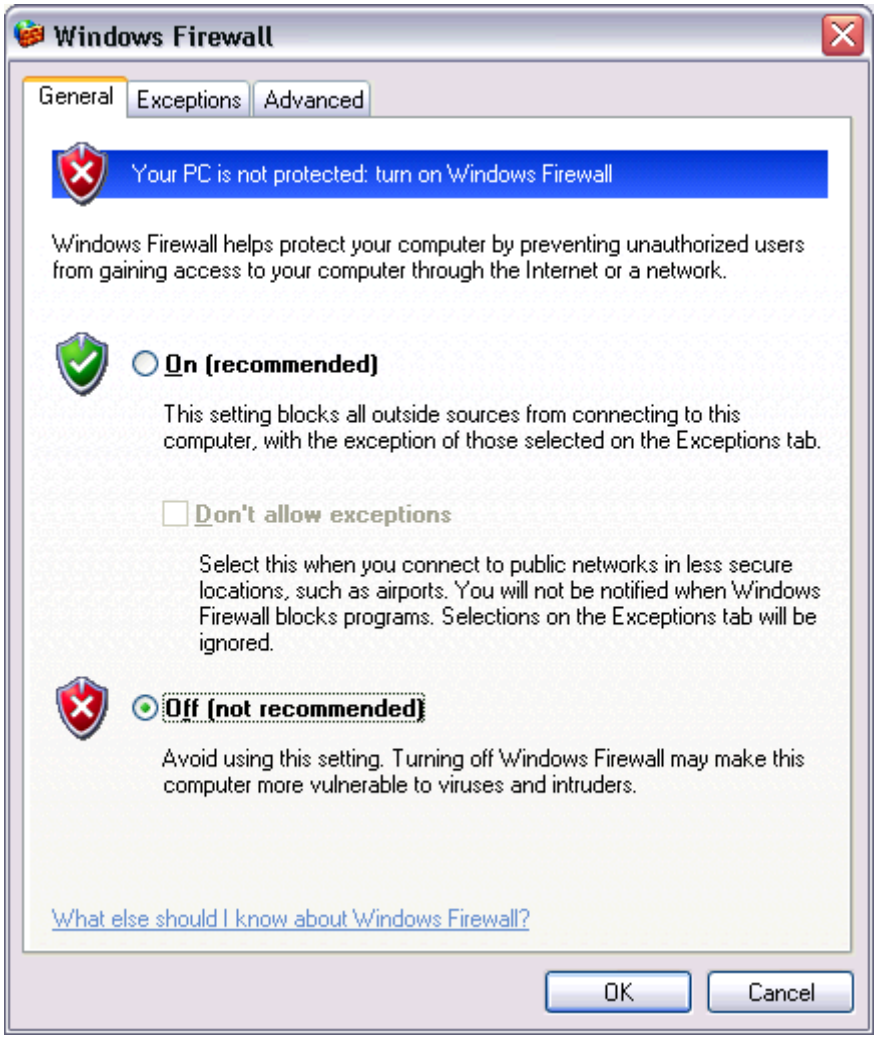
4. If one or both services are not running, start them manually. To start the service, right click it and select **Start** from the context menu. The selected service is started.

To quickly access Windows Services, press **Windows+R,** type **services.msc** in the Run text box and press **Enter.**

Disabling Windows XP/Vista Firewall

To disable Windows XP Firewall:

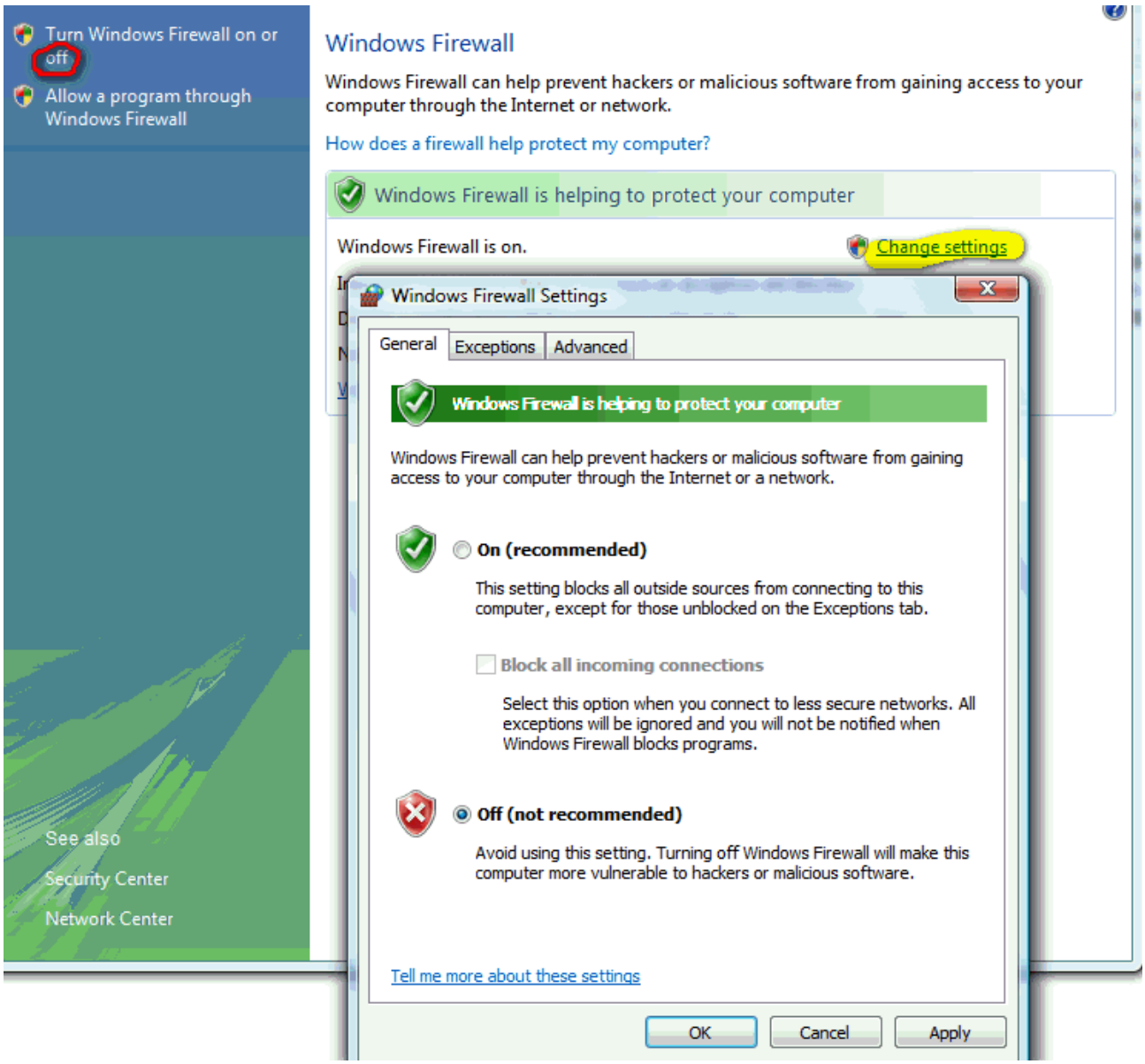
1. Select **Start > Control Panel > Windows Firewall**.
2. The Windows Firewall window opens.


Windows Firewall
General
Exceptions
Advanced
Your PC is not protected: turn on Windows Firewall
Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.
On (recommended)
This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.
Don't allow exceptions
Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.
Off (not recommended)
Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.
What else should I know about Windows Firewall?
OK
Cancel

3. Select **Off (not recommended)** and click **OK**.

To disable Windows Vista Firewall:

1. Select **Start > Control Panel > Security > Windows Firewall**.
2. Click **Turn Windows Firewall on or off**. Enter your administrator password if prompted to do so.


Turn Windows Firewall on or off
Allow a program through Windows Firewall
See also
Security Center
Network Center
Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or network.
How does a firewall help protect my computer?
Windows Firewall is helping to protect your computer
Windows Firewall is on.
Change settings
Windows Firewall Settings
General
Exceptions
Advanced
Windows Firewall is helping to protect your computer
Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.
On (recommended)
This setting blocks all outside sources from connecting to this computer, except for those unblocked on the Exceptions tab.
Block all incoming connections
Select this option when you connect to less secure networks. All exceptions will be ignored and you will not be notified when Windows Firewall blocks programs.
Off (not recommended)
Avoid using this setting. Turning off Windows Firewall will make this computer more vulnerable to hackers or malicious software.
Tell me more about these settings
OK
Cancel
Apply

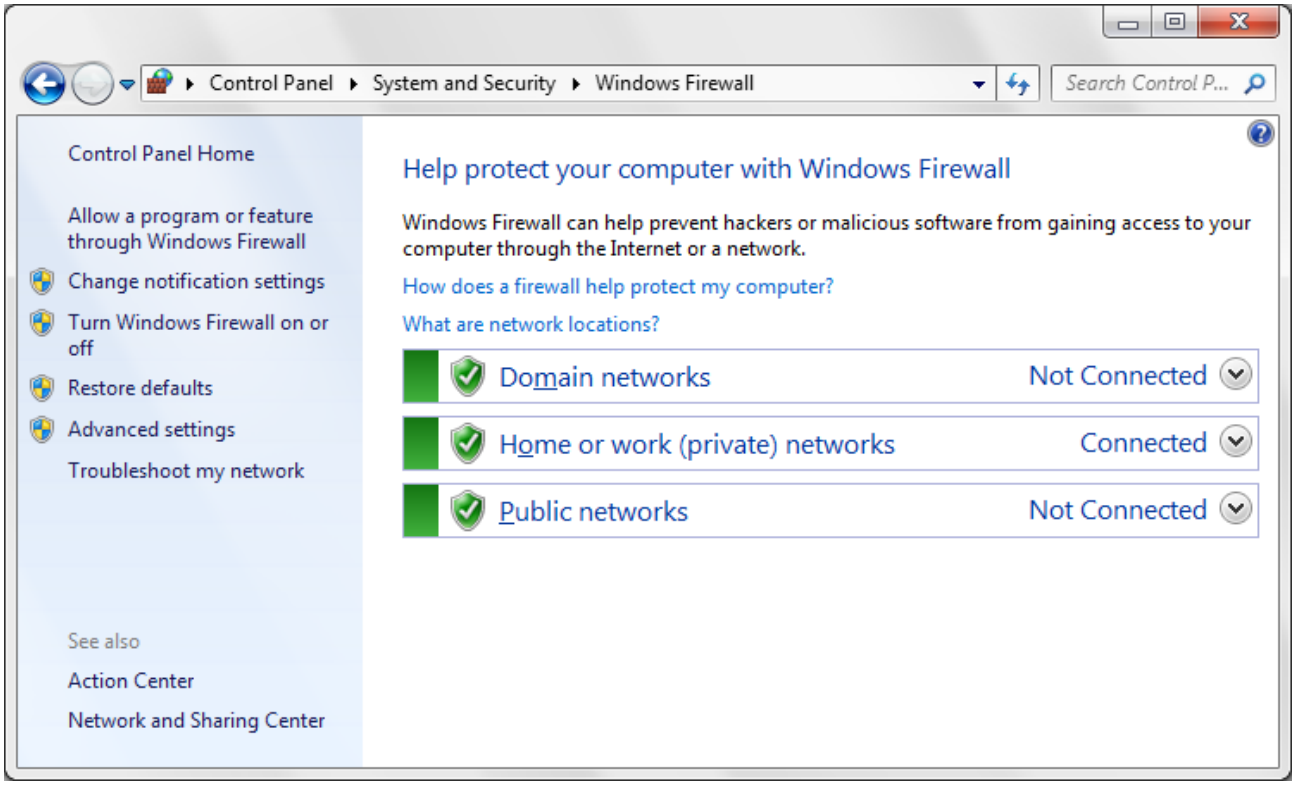
3. In the Windows Firewall Settings window, select **Off (not recommended)** and click **OK**.

Setting Up Windows 7/8 Firewall

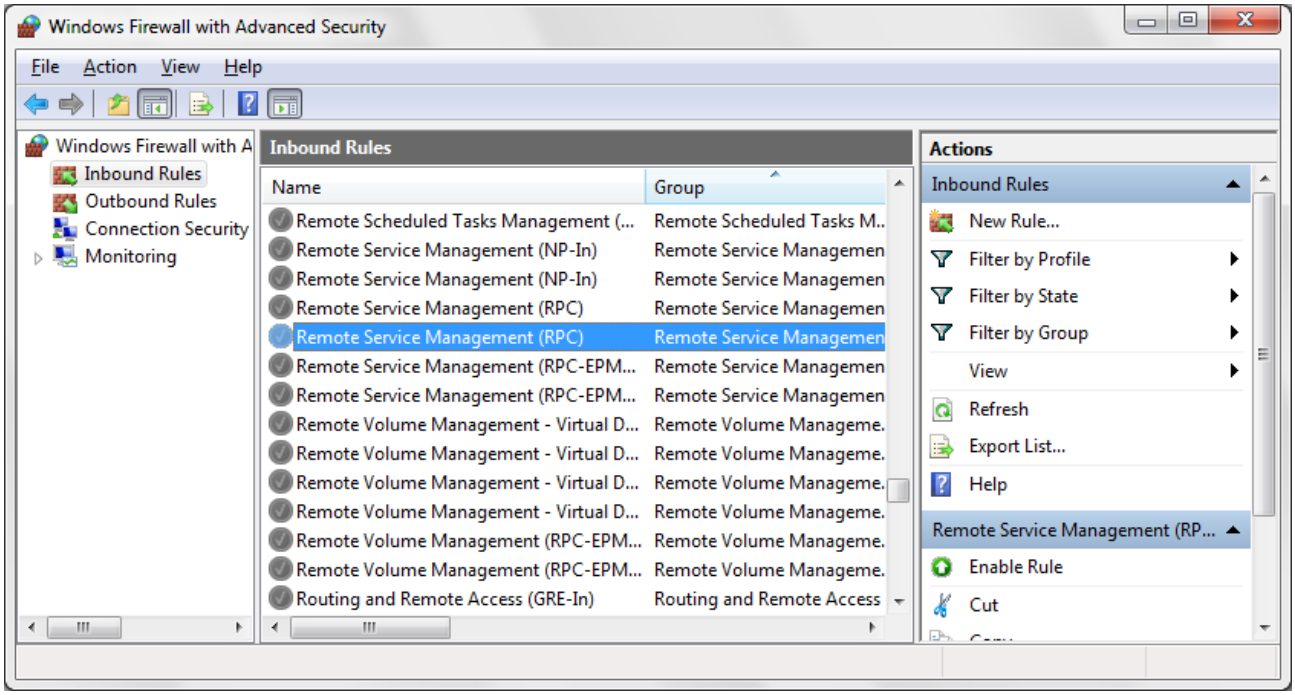
It is not necessary to disable the Windows Firewall in Windows 7 and Windows Server 2008. For successful remote installation of Desktop Surveillance Clients, you have to allow inbound connections in the Remote Service Management (RPC) rule for the remote computers.

To enable inbound connections for the Remote Management Service (RPC), do the following:

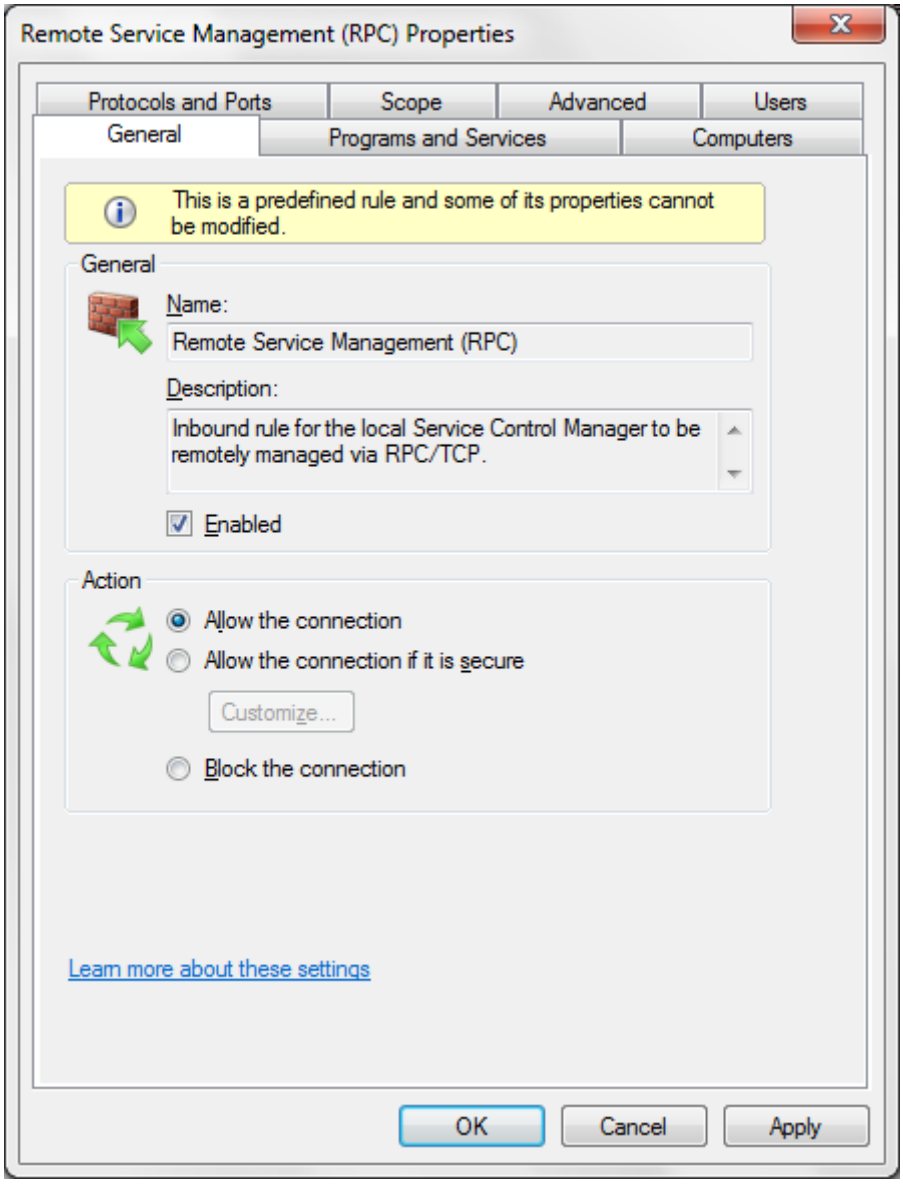
1. Select **Start > Control Panel > System and Security > Windows Firewall**.
2. The Windows Firewall window opens.


Control Panel ▸ System and Security ▸ Windows Firewall
Search Control P...
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center
Help protect your computer with Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.
How does a firewall help protect my computer?
What are network locations?
Domain networks
Not Connected
Home or work (private) networks
Connected
Public networks
Not Connected

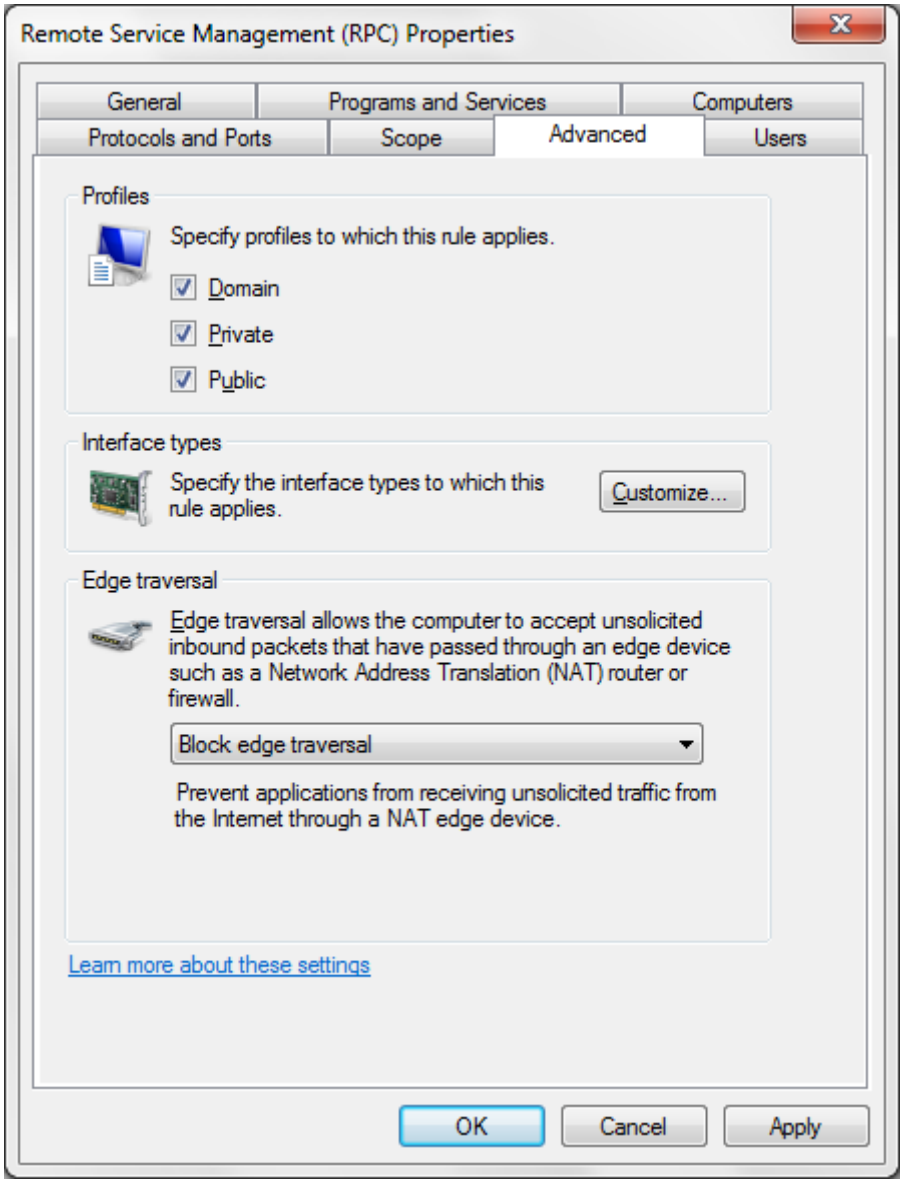
3. Click **Advanced settings**. The Windows Firewall with Advanced Security window opens.
4. Click **Inbound Rules** and then double click the **Remote Service Management (RPC)** rule in the rules list.



5. The Remote Service Management (RPC) Properties window opens.



6. In the **General** tab, select **Enabled** under **General** and click **Allow the connection** under **Action**.
7. In the **Advanced** tab, under **Profiles**, select the profile of the network used for connecting remote computers and the Desktop Surveillance Server.



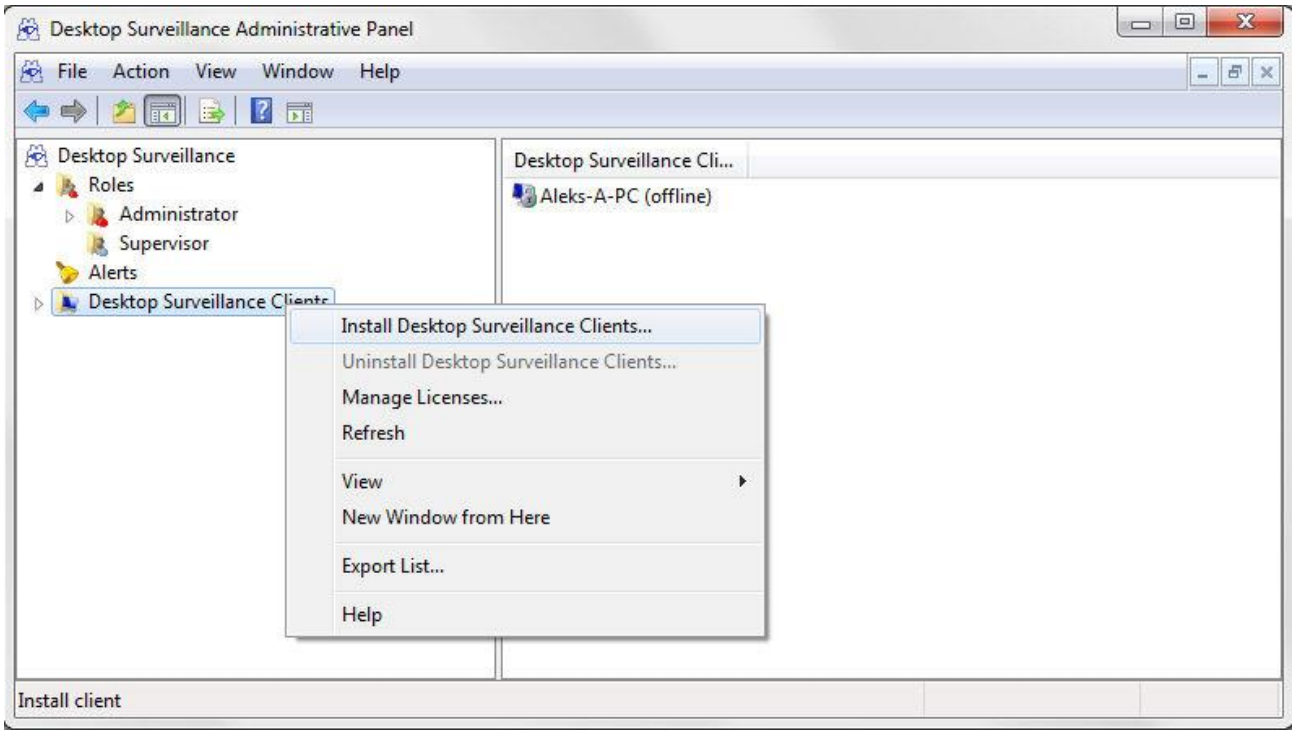
8. Click **Apply** and then **OK** to save the settings and close the Properties window.
9. Close the Windows Firewall window.
10. Create an inbound rule for Server executable.

Installing Desktop Surveillance Clients via Administrative Panel

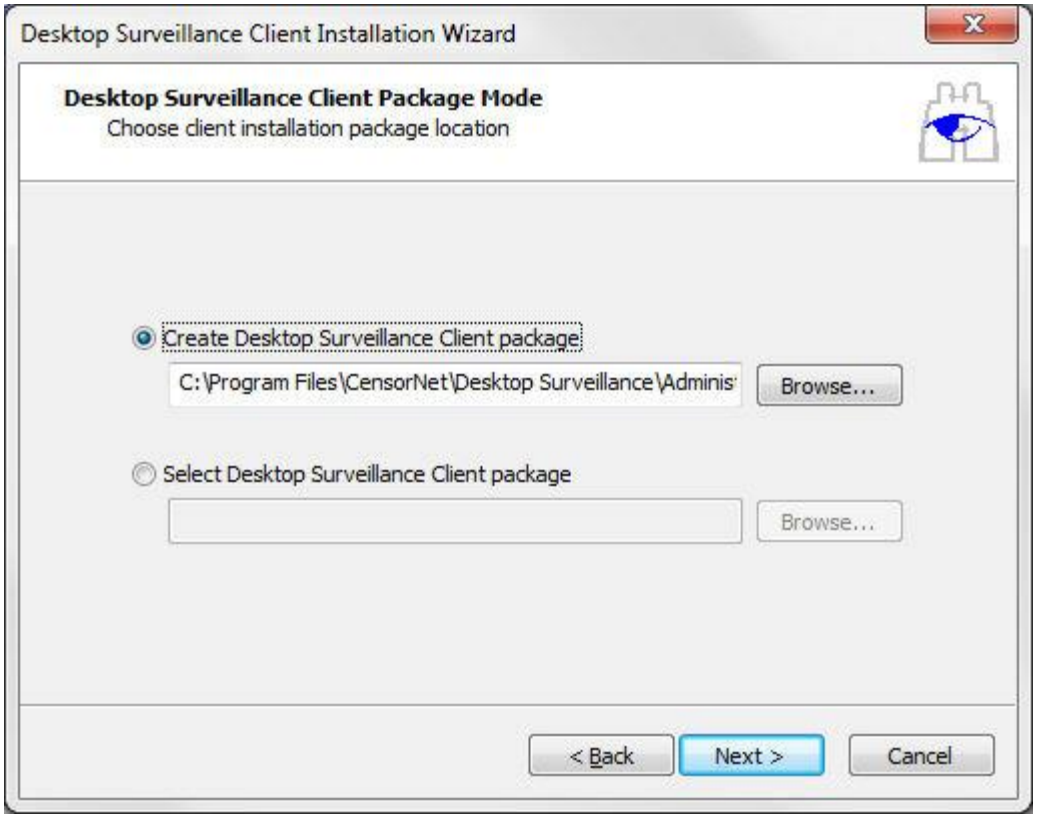
To perform the remote Client installation via Desktop Surveillance Administrative Panel, do the following:

1. Start the Desktop Surveillance Administrative Panel.
2. Select Desktop Surveillance Clients in the navigation pane or details pane.

3. Click **Action** and select **Install Desktop Surveillance Client** or right-click and select **Install Desktop Surveillance Clients**.

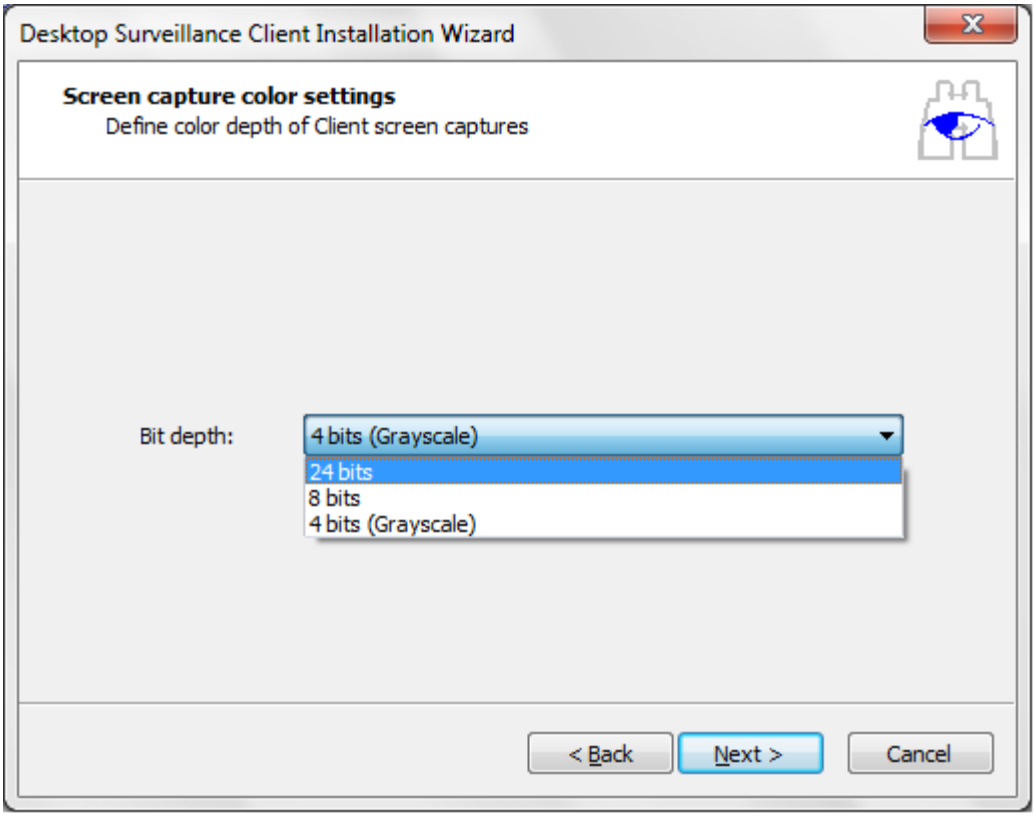


4. The **Desktop Surveillance Client Installation Wizard** opens. Click **Next** on the Welcome page.
5. On the **Desktop Surveillance Client Package Mode** page, select one of two options and click **Next**:
    - **Create Desktop Surveillance Client package**: Use this option if you haven't performed a remote installation yet. Type the path to the newly created package or click **Browse** and navigate to it.
    - **Select Desktop Surveillance Client package**: Use this option if you have performed a remote installation already. Type the path to the installation package or click **Browse** and navigate to it.

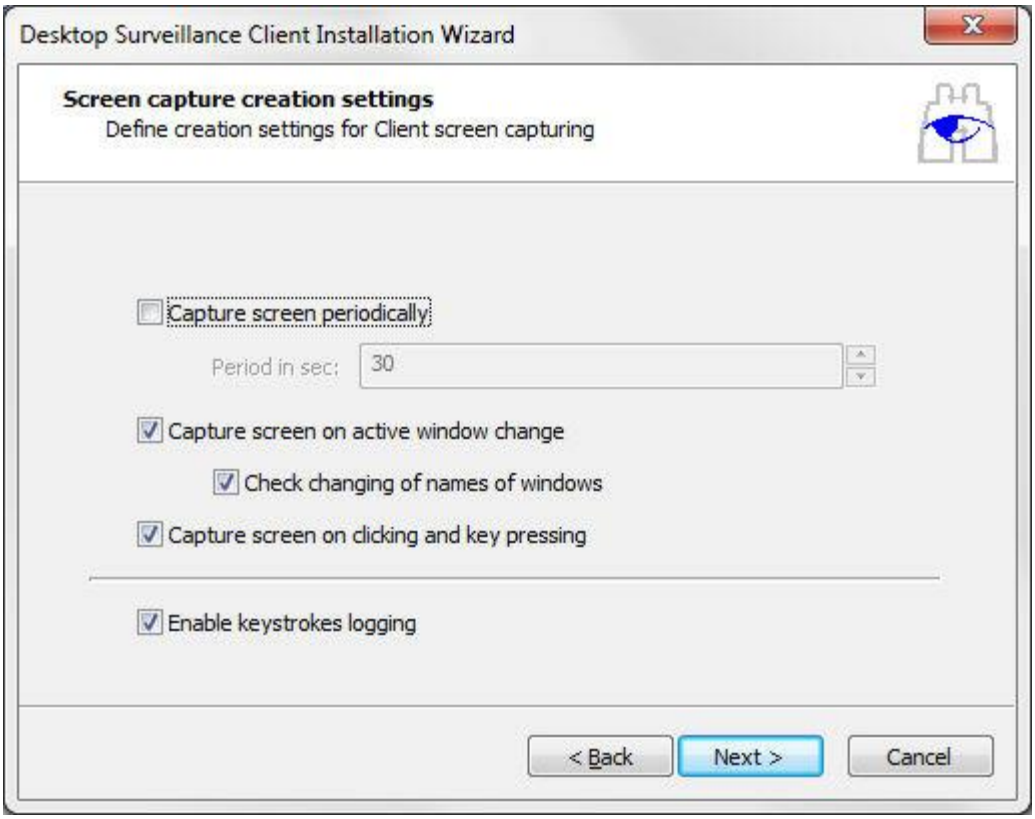


NOTE: If you select the Select Desktop Surveillance Client package option, steps 6,7,8 will be omitted.

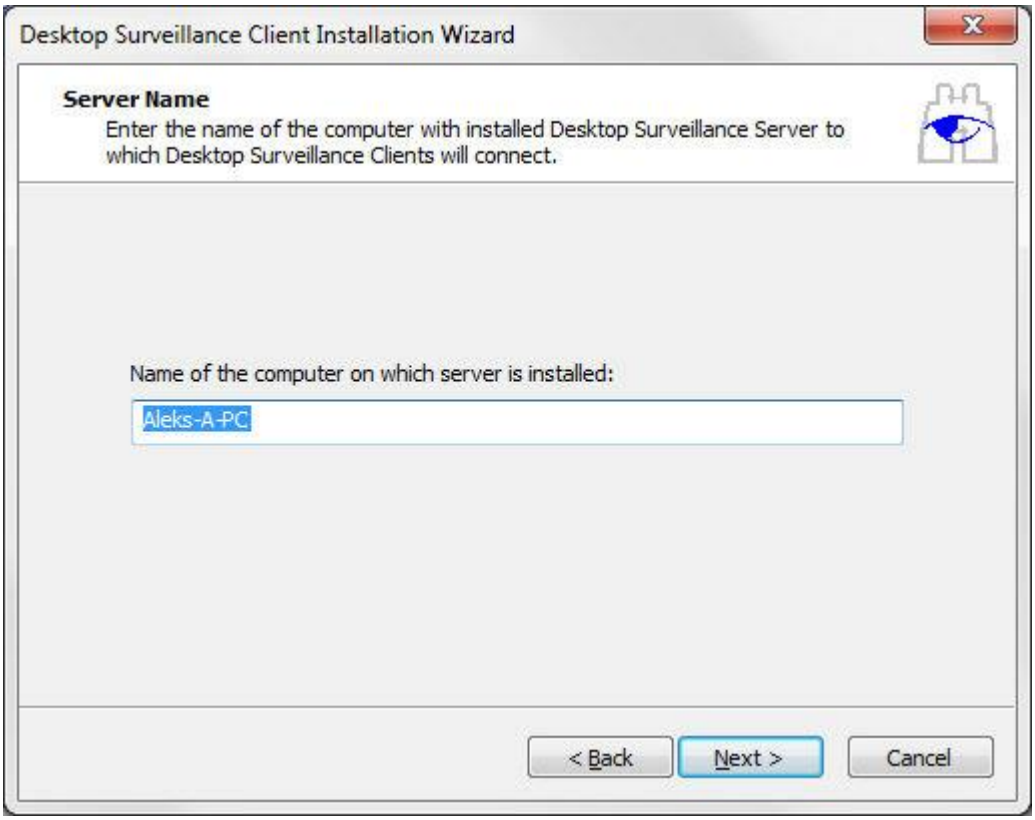
6. On the **Screen capture color settings** page, select the color depth for the created screen captures and click **Next**.



7. On the **Screen capture creation settings** page, define the frequency with which the screen captures will be created. Click **Next.**

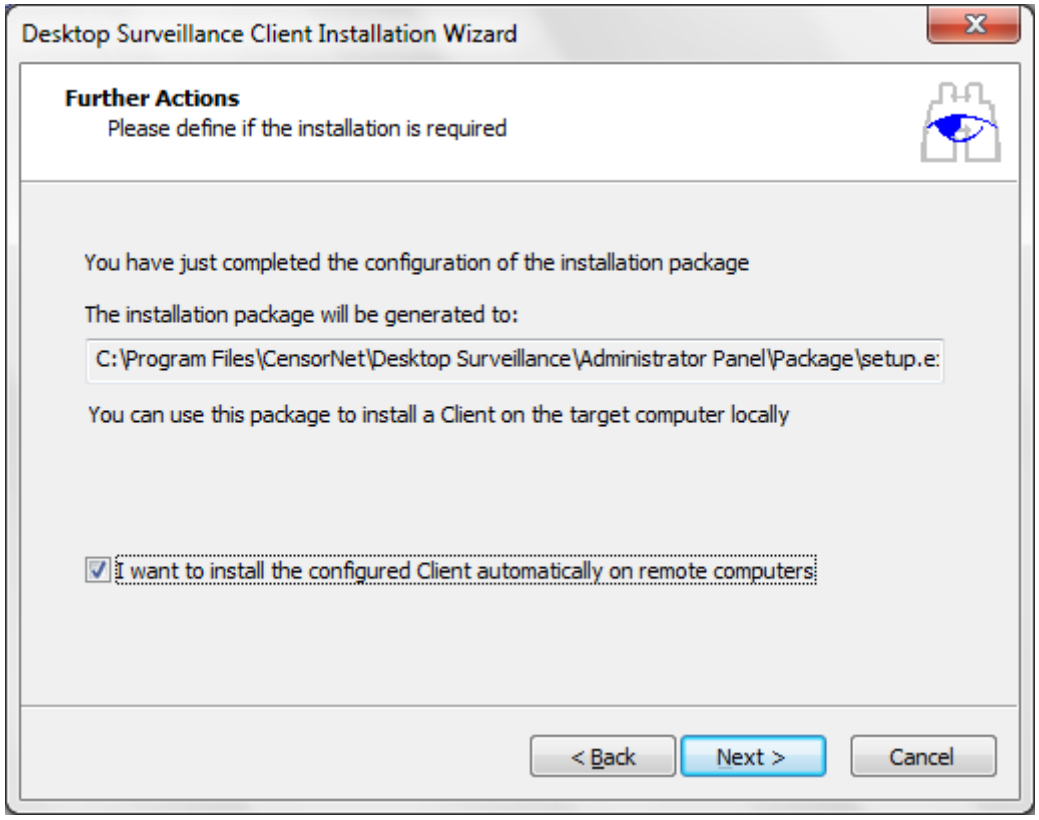

Desktop Surveillance Client Installation Wizard
Screen capture creation settings
Define creation settings for Client screen capturing
Capture screen periodically
Period in sec:
30
Capture screen on active window change
Check changing of names of windows
Capture screen on clicking and key pressing
Enable keystrokes logging
< Back
Next >
Cancel

8. On the **Server Name** page, type the name or the IP-address of the computer on which the Desktop Surveillance Server and Administrative Panel are installed. Clients will connect to this server and the received screen captures will be stored on its computer. Click **Next.**

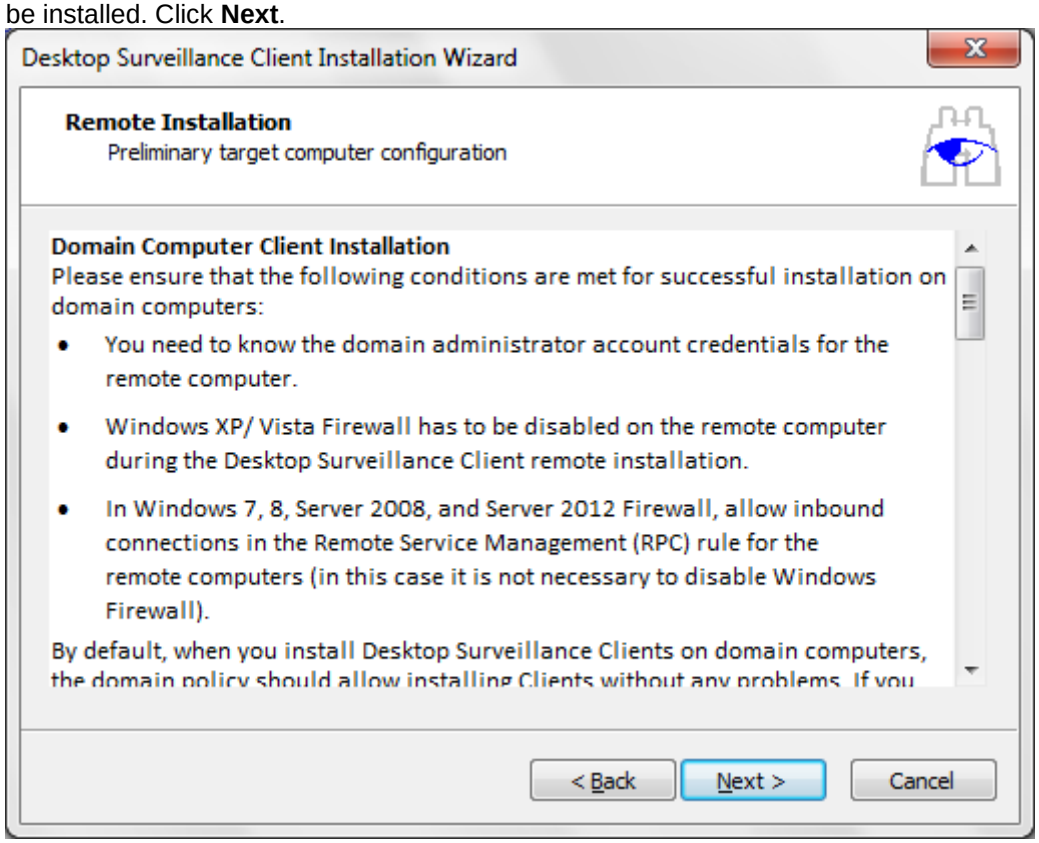

Desktop Surveillance Client Installation Wizard
Server Name
Enter the name of the computer with installed Desktop Surveillance Server to which Desktop Surveillance Clients will connect.
Name of the computer on which server is installed:
Aleks-A-PC
< Back
Next >
Cancel

Note: The server IP address has to be static for clients to connect to it successfully. Unique external IP addresses should be used for cloud-based servers.

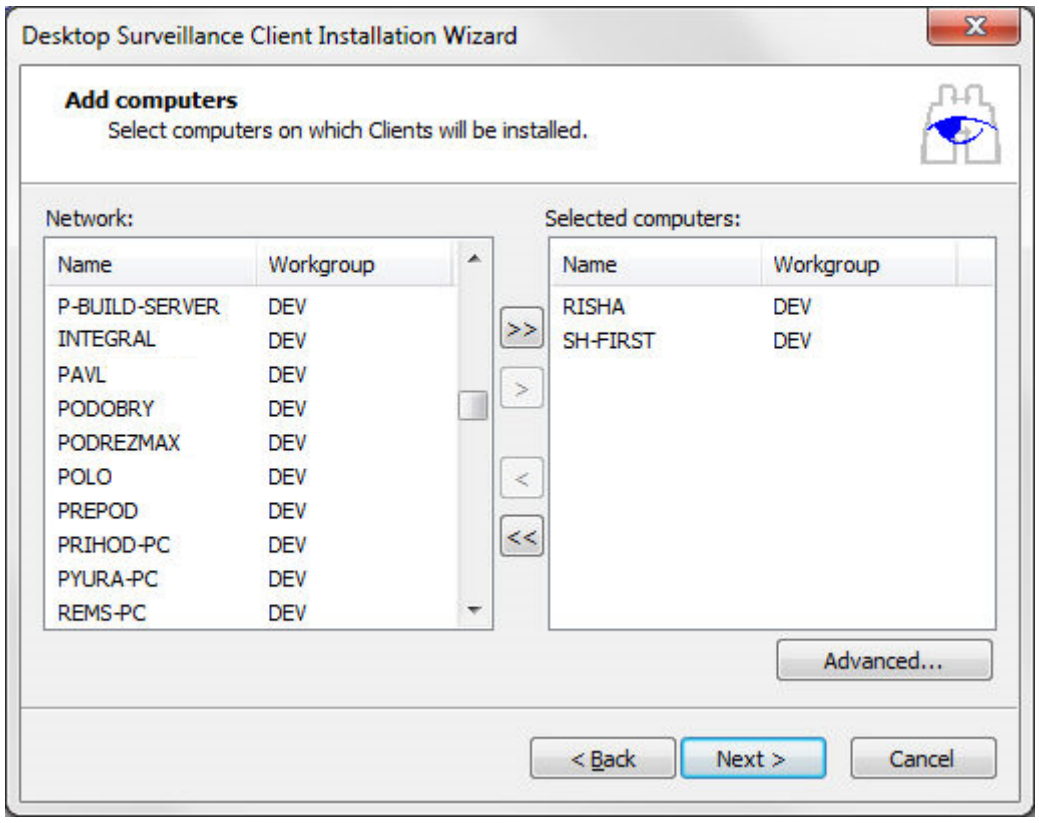
9. On the **Further Actions** page, check the location to which the installation package will be saved and select the **I want to install the configured Client automatically on remote computers** option. Click **Next**.


Desktop Surveillance Client Installation Wizard
Further Actions
Please define if the installation is required
You have just completed the configuration of the installation package
The installation package will be generated to:
C:\Program Files\CensorNet\Desktop Surveillance\Administrator Panel\Package\setup.e:
You can use this package to install a Client on the target computer locally
I want to install the configured Client automatically on remote computers
< Back
Next >
Cancel

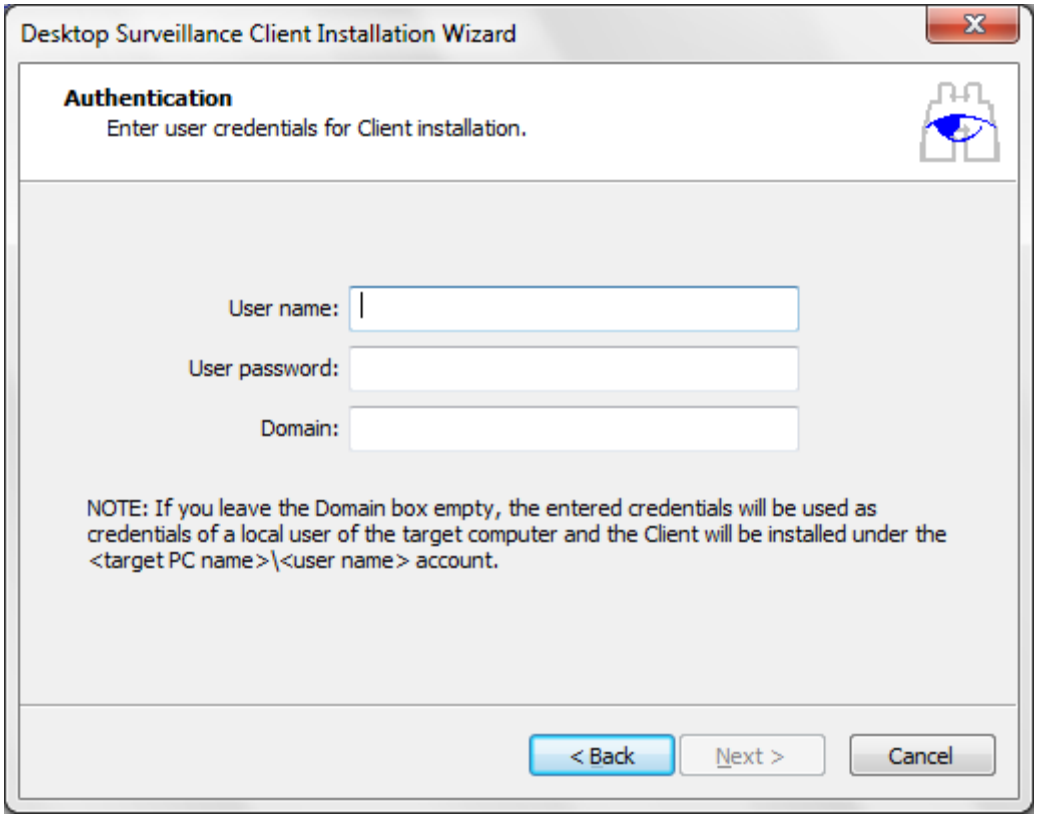
10. On the **Remote Installation** page, read the information that will help you to install Clients on remote computers successfully and make sure that all conditions are met on computers on which Clients are to be installed. Click **Next**.


Desktop Surveillance Client Installation Wizard
Remote Installation
Preliminary target computer configuration
Domain Computer Client Installation
Please ensure that the following conditions are met for successful installation on domain computers:
You need to know the domain administrator account credentials for the remote computer.
Windows XP/ Vista Firewall has to be disabled on the remote computer during the Desktop Surveillance Client remote installation.
In Windows 7, 8, Server 2008, and Server 2012 Firewall, allow inbound connections in the Remote Service Management (RPC) rule for the remote computers (in this case it is not necessary to disable Windows Firewall).
By default, when you install Desktop Surveillance Clients on domain computers, the domain policy should allow installing Clients without any problems. If you
< Back
Next >
Cancel

11. On the **Add computers** page, select hosts on which Clients are to be installed. Click **Next.**



12. On the **Authentication** page, enter the administrator credentials under which the Clients are to be installed and then click **Next**:
    - If the computers are in a domain, enter the domain name and domain Administrator account credentials.
    - If the computers are in workgroup, leave the **Domain** box empty and enter the credentials of a local Administrator for target computers.
      NOTE: All workgroup computers must have the same Administrator account credentials. Otherwise use installation via installation package method to deploy Desktop Surveillance Clients.



13. Package creation starts. As soon as the package is created, it is deployed on the selected host computers and the Client is installed on them.
14. Wait for the wizard to complete the installation and click **Finish**.

Installing Clients via Installation Package

You can install Desktop Surveillance Clients via the installation package in 2 ways:

- via the administrative panel using the formerly created package
- by copying the package to the remote computer and starting it there.

To create an installation package:

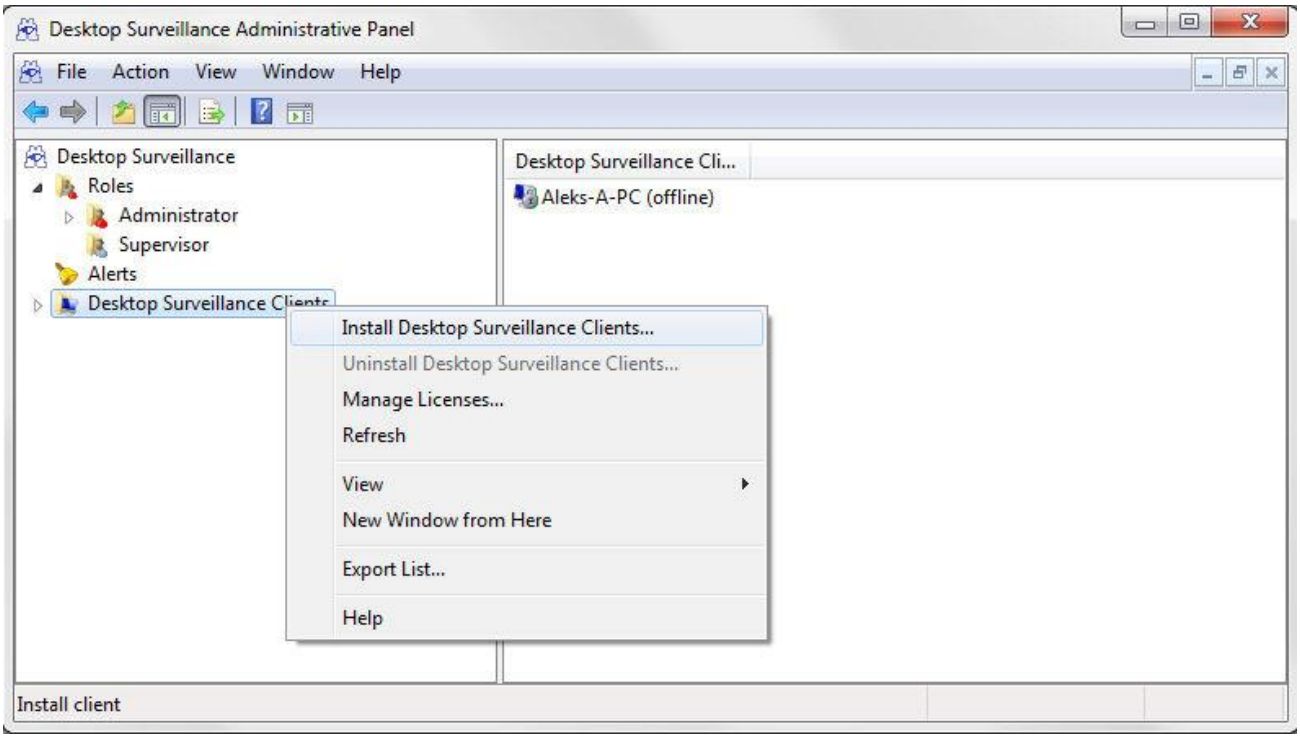
NOTE: Steps are the same as steps 5-9 of the remote Client installation instructions.

1. Start the Desktop Surveillance Administrative Panel.
2. Select Desktop Surveillance Clients in the navigation pane or details pane.
3. Click **Action** and select **Install Desktop Surveillance Client** or right-click and select **Install Desktop Surveillance Client**.
4. The **Desktop Surveillance Client Installation Wizard** opens. Click **Next** on the Welcome page.
5. On the **Desktop Surveillance Client Package Mode** page, select **Create Desktop Surveillance Client package** and click **Browse** to select a folder to which it will be saved, and then click **Next**.

6. On the **Screen capture color settings** page, select the color depth for the created screen captures and click **Next**.
7. On the **Screen capture creation settings** page, define the frequency with which the screen captures will be created. Click **Next.**
8. On the **Server Name** page, type the name or the IP-address of the computer on which the Desktop Surveillance Server and Administrative Panel are installed. Clients will connect to this server and the received screen captures will be stored on its computer. Click **Next.**
   NOTE: The server IP address has to be static for Clients to connect to it successfully. Unique external IP addresses should be used for cloud-based servers.
9. On the **Further Actions** page, check the location to which the installation package will be saved and clear the **I want to install the configured Client automatically on remote computers** option. Click **Next**.
10. Package creation starts. As soon as the package creation is finished, click **Finish**.

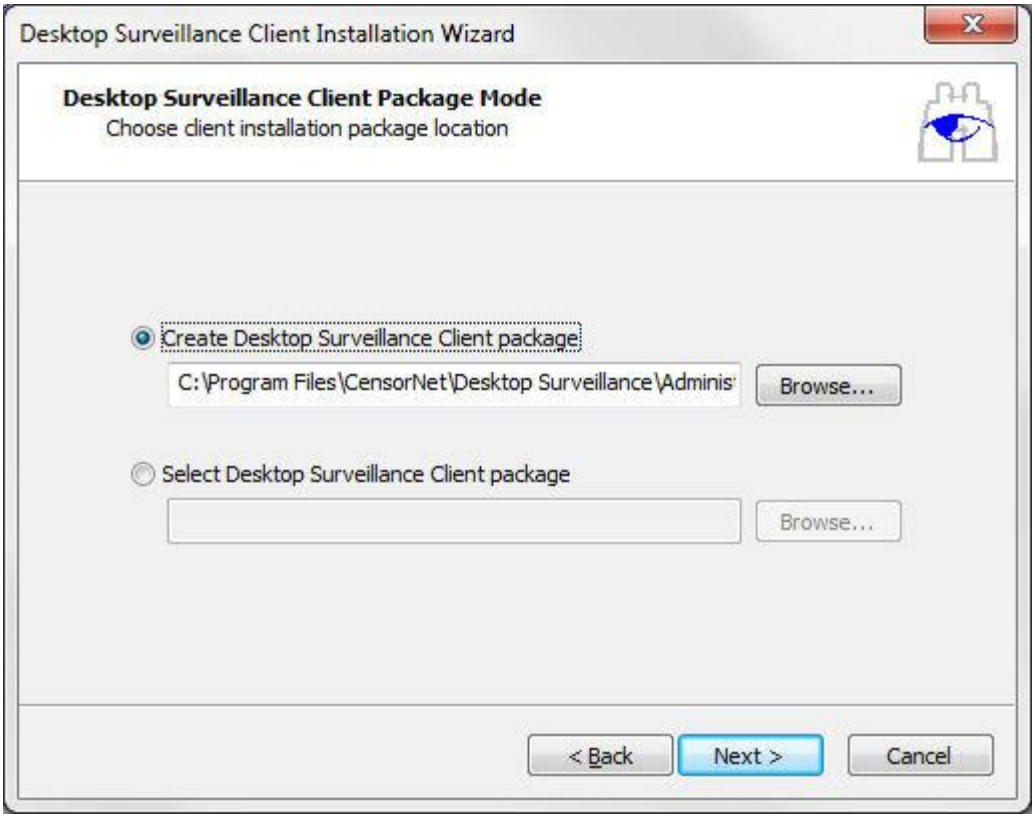
To install Desktop Surveillance Client via Administrative Panel using installation package, do the following:

1. Start the **Desktop Surveillance Administrative Panel**.
2. Select the **Desktop Surveillance Clients** node to the right of the window.
3. Right click and select **Install Desktop Surveillance Client**.



4. The **Desktop Surveillance Client Installation Wizard** opens. Click **Next** on the Welcome page.

5. On the **Desktop Surveillance Client Package Mode** page, choose the **Select Desktop Surveillance Client package** option and click **Browse**.



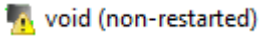
6. Navigate to the formerly created package and select it. Click **Next**.
7. Continue the installation as described in common remote installation.

To install Desktop Surveillance Client using the installation package on the target computer:

1. Copy the package to the remote computer and start it under the Administrator account. By default, the created package is saved to the following directory: **<Desktop Surveillance installation folder>\Administrative Panel\Package**.
2. After the package is deployed, the name of the required computer appears as a sub-node of the **Desktop Surveillance Clients** node in the **Desktop Surveillance Administrative Panel**.

Updating the Desktop Surveillance Clients

The Desktop Surveillance Client updating is performed automatically when a Client connects to the Server of a newer version. As soon as updates are applied to a Client, you'll see a warning icon and a **non-restarted** status message near the Client name indicating that a reboot of the Client computer is required.



NOTE: Not restarted Clients do not stop the monitoring and all features of the old Client are still available to them, but new features will not be available until the Client computer is rebooted.

After a reboot you will also be able to access the monitored data of the old Client.

In some cases, if you install a newer version of the Desktop Surveillance Server, Clients of very old versions will not be able to update and you will see the **unable to update** status message near the Client name. In this case you need to uninstall the old Client and install a new version of a Client.

Cloning a Virtual Machine with Installed Client

Each Client has its own unique ID, which it receives when it connects to the Server. When you prepare a virtual machine, which is to be monitored by Desktop Surveillance, for cloning, you need to remove the Client ID to ensure the proper Client connection to Server.

To remove the Client ID:

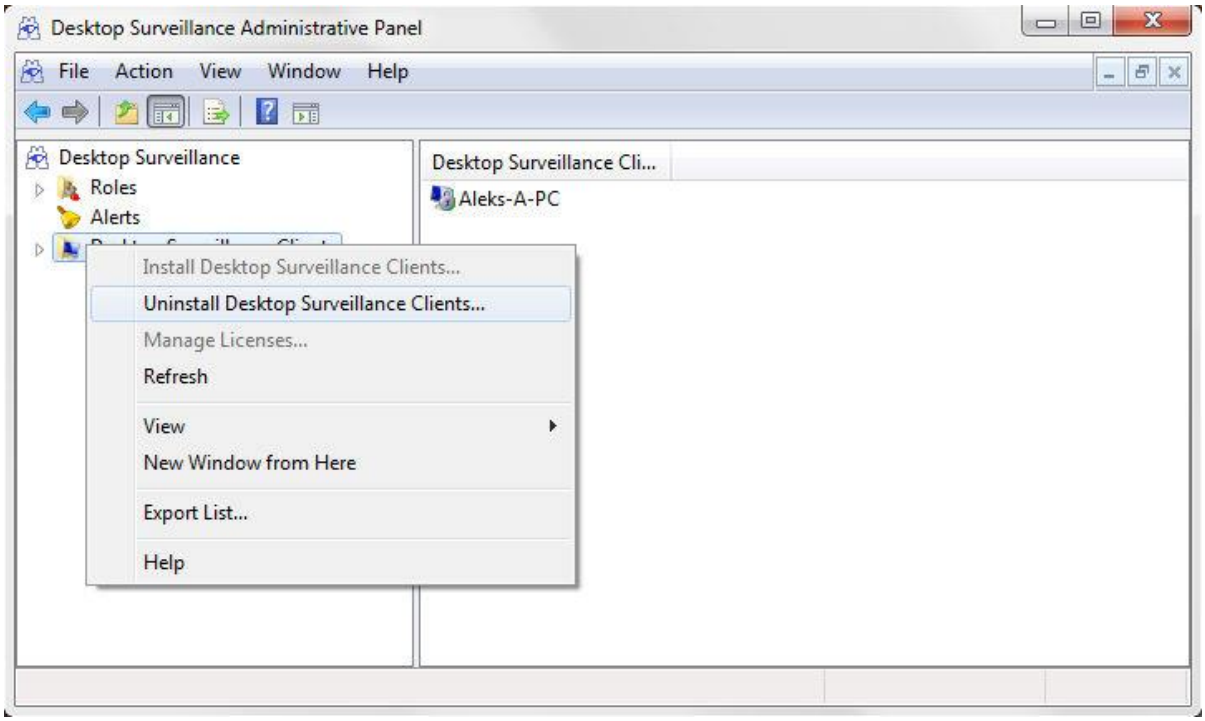
1. Open the Windows Registry Editor.
2. In the Registry Editor window, select the following key **HKEY_LOCAL_MACHINE\SOFTWARE\CensorNet\Desktop Surveillance.**
3. Double-click the **AgentGUID** value or select it and click **Modify** in the right-click menu.
4. Remove the ID from the **Value Data** box.
5. Click **OK**.

Uninstalling Clients

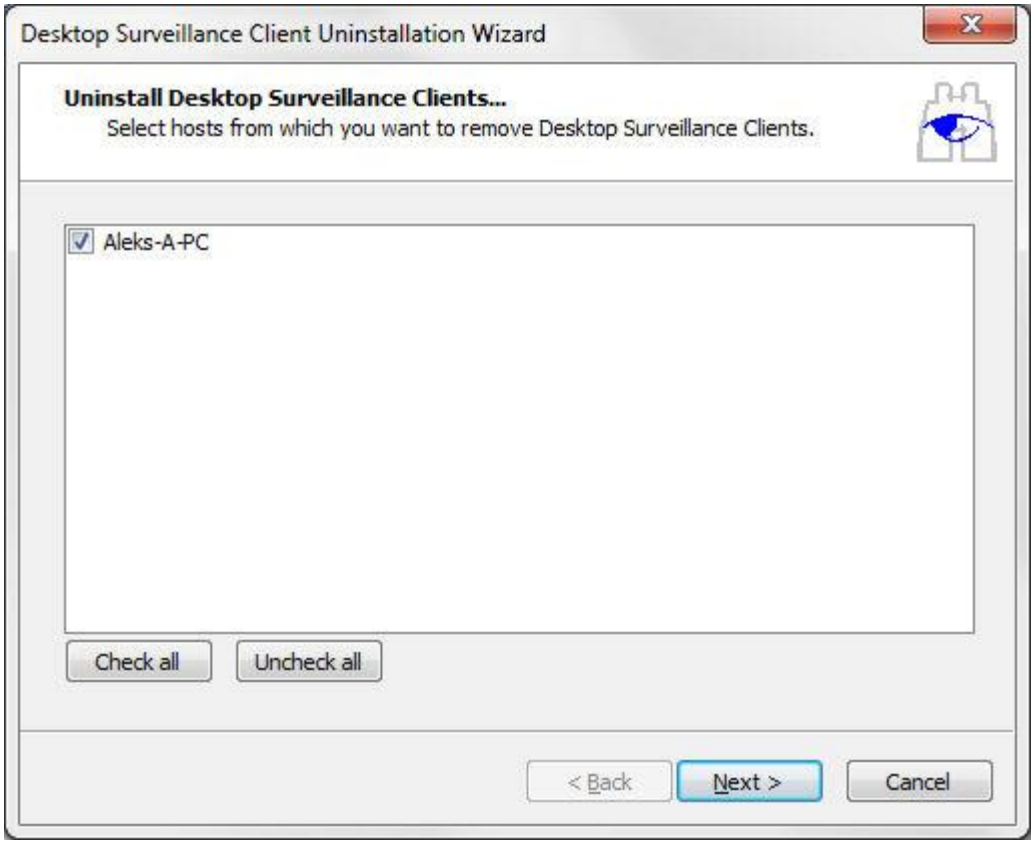
You can uninstall more than one Desktop Surveillance Client from selected host(s).

To uninstall the Client:

1. Start the CensorNet Desktop Surveillance Administrative Panel.
2. Select **Desktop Surveillance Clients** in the navigation pane or details pane.
3. Select **Action > Uninstall DesktopSurveillance Client** or right-click and select **Uninstall Desktop Surveillance Client**.



4. The **Desktop Surveillance Client Uninstallation Wizard** opens.

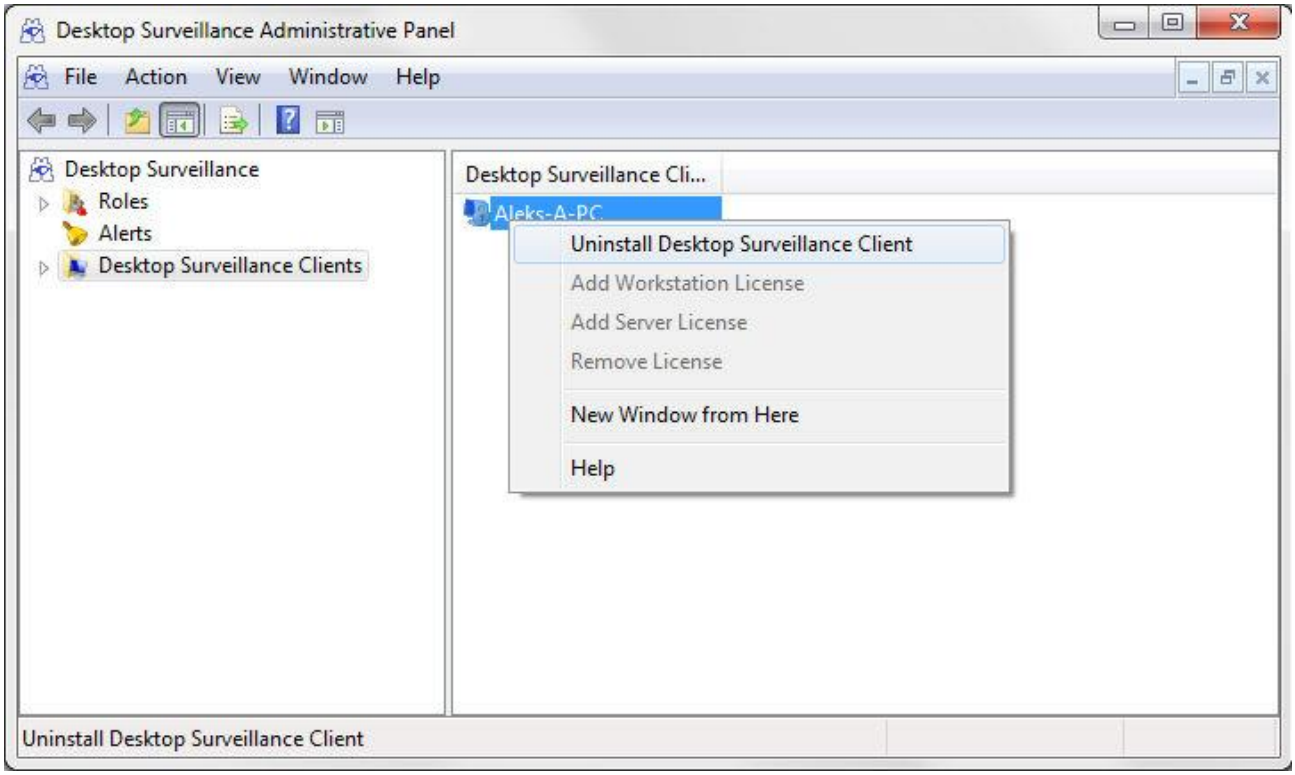


5. Select the hosts from which Clients will be uninstalled. Select the checkbox near the name of the corresponding host. You can use the **Check All/Uncheck All** buttons to select/disselect all Clients. Click **Next**.
6. The uninstallation process starts. After the uninstallation finishes, click **Finish** to exit the wizard.

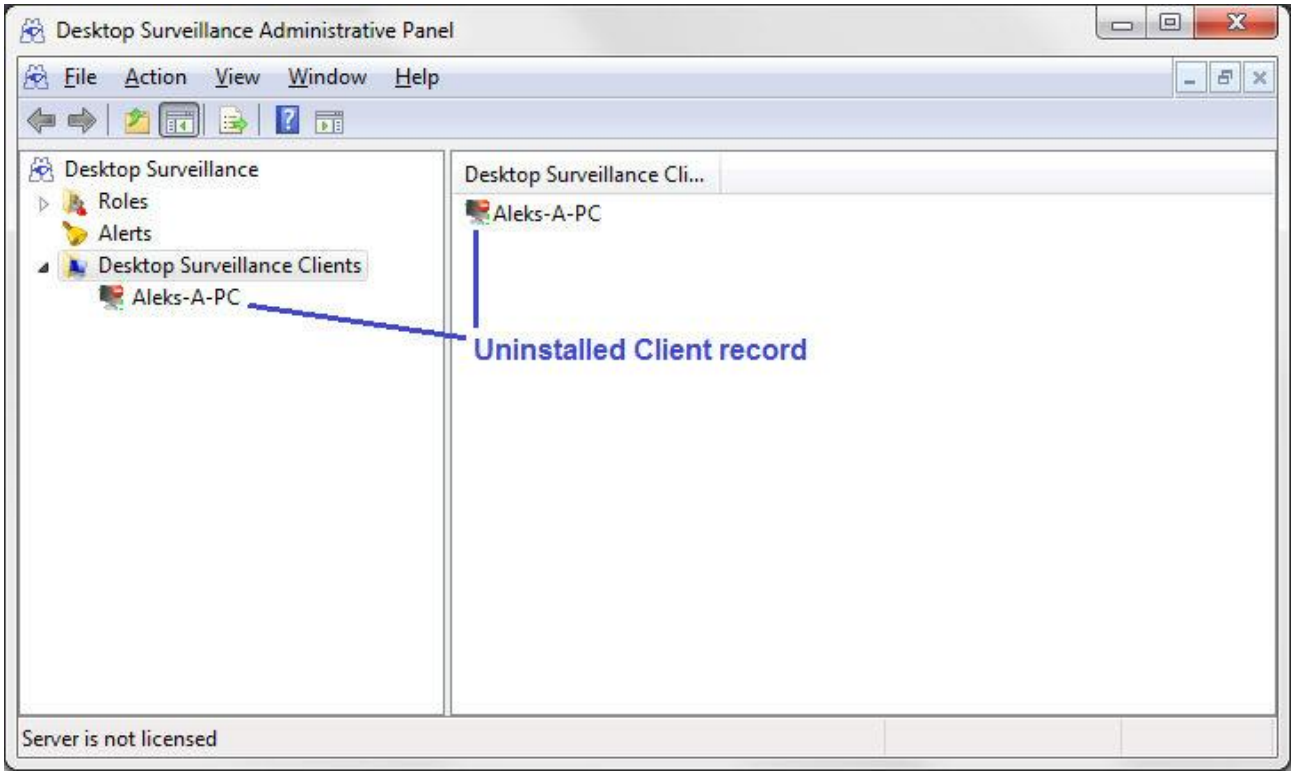
NOTE: You can uninstall a single client by clicking Uninstall Desktop Surveillance Client in its context menu.

To uninstall a single Client:

1. Start the Administrative Panel.
2. Select **Desktop Surveillance Clients** list in the navigation pane.
3. Right click the target Client and select **Uninstall Desktop Surveillance Client**.



4. Confirm the Client uninstallation.
5. If the Client had transferred any user activity records before it was removed, the corresponding host remains in the list of Corporate Security Monitor Clients marked as uninstalled. The respective user activity records are kept stored on the Corporate Security Monitor Server.



Licensing

General Licensing Information

To start receiving information from Desktop Surveillance Clients, you have to assign **licenses** to them. Two types of licenses are available:

- **Workstation license:** Clients with this license monitor only one session, either remote or local, on the investigated computer.
  NOTE: Licenses of the workstation type cannot be assigned to a computer with Server OS.
- **Server license:** Clients with this license monitor unlimited number of remote sessions and any local sessions on the investigated computer. Remote sessions include Remote Desktop sessions, terminal sessions, etc.

Each client can have only one license assigned, either workstation or server.

Initially, when you start the Desktop Surveillance Server for the first time on a computer, you have an embedded trial serial key, which allows you to use 5 workstation licenses and 1 server license for 30 days.

To use the Desktop Surveillance permanently and with greater number of licenses, you have to license it with purchased serial keys.

NOTE: After activation of any serial key, the embedded trial key expires.

Two types of serial keys are available:

- **Standard serial keys:** These keys allow you to use licenses they contain during the unlimited period of time and allow you to update the product during 12 months from activation.
- **Trial serial keys:** These keys allow you to use the licenses they contain during 30 days from activation and update the product during this period.

Each serial key includes the following parameters:

- Subscription period
- Server licenses for Desktop Surveillance Clients
- Workstation licenses for Desktop Surveillance Clients

You can either activate serial keys online or add activated serial keys if you have no Internet connection on a computer with installed Desktop Surveillance Server. Contact your vendor for information on purchasing serial keys.

Please note, after the activation, serial keys are bound to a specific computer and cannot be used on another computer.

About Subscription

A subscription is a period that defines what updates can be applied to your copy of the product. Updates are defined by their release date. After the subscription expires, you can still assign licenses to Clients, but you won't be able to update Desktop Surveillance to versions released after the subscription expiration date.

The subscription end date is defined during the serial key activation (either via Desktop Surveillance Administrative Panel or on the vendor's site). It is calculated using a serial key with the longest subscription period.

For example, if you activate two keys, one with a 30 days subscription period and one with a

12 months subscription period, simultaneously, the subscription end date will be set to 12 months from the activation date.

When a new serial key is being activated, the subscription period is prolonged accordingly. Please note, if the current subscription period is longer than the one of a key being activated, current subscription period doesn't change. For example, if you activate a key with 12 months subscription period after a key with 30 days subscription period, the subscription end date will be set to 12 months since the activation date. But if you activate a key with 30 days subscription period after a key with 12 months subscription period, the subscription end date will not change.

If your subscription expires, you can purchase a special **subscription extension serial key**, which does not contain any keys, but extends your subscription period, or you can activate any other serial key

To view the subscription expiration date, select **Action > Manage Serial Keys** or right-click the **Desktop Surveillance** node and select **Manage Serial Keys**.

Activating Serial Keys Online

To activate purchased serial keys online, do the following:

1. Make sure you have an active Internet connection on the computer with installed Desktop Surveillance Server.
2. Start the Desktop Surveillance Administrative Panel and select the **Desktop Surveillance** node.
3. Select **Action > Manage Serial Keys,** or right-click the **Desktop Surveillance** node and select **Manage Serial Keys**.
4. The **Desktop Surveillance Serial Keys Management** window opens.
5. Click **Activate keys online**.
6. The **Desktop Surveillance Serial Keys Online Activation** window opens.
7. Enter serial keys to be activated separating them with spaces or paragraphs and click **Activate**.
8. The progress of serial key activation is displayed in the **Desktop Surveillance Serial Key Activation** window.

9. If serial keys are successfully activated, you will see a confirmation message. Click **Close** in the message.
10. The newly activated serial keys are highlighted in bold in the **Desktop Surveillance Serial Keys Management** window.
11. The number of available server and workstation licenses and the subscription end date change.
12. Click **Close** in the **Desktop Surveillance Serial Keys Management** window.

Adding Activated Serial Keys Offline

If you have no Internet connection on a computer on which the serial keys are to be activated, you can activate them on the license site and then add the activated serial keys offline. For more information, send an email to sales@censornet.com

To add activated serial keys in offline mode, do the following:

1. Start the Desktop Surveillance Administrative Panel and select the **Desktop Surveillance** node.
2. Select **Action > Manage Serial Keys,** or right-click the **Desktop Surveillance** node and select **Manage Serial Keys**.
3. The **Desktop Surveillance Serial Keys Management** window opens.
4. Click **Add activated keys**.
5. The **Desktop Surveillance Activated Serial Keys Offline Adding** window opens.
6. Enter the path to the activatedKeys.txt file with activated serial keys in the empty text box or click **Browse** and navigate to the required file.
7. Click **Add**.
8. The newly added serial keys are highlighted in bold in the **Desktop Surveillance Serial Keys Management** window.
9. The number of available server and workstation licenses and the subscription end date change.
10. Click **Close** in the **Desktop Surveillance Serial Keys Management** window.

Viewing License State

You can view the information on serial keys you have activated or added and license details in the Desktop Surveillance Serial Keys Management window.

To view the license state, select **Action > Manage Serial Keys** or right-click the **Desktop Surveillance** node and select **Manage Serial Keys**.

The following information is displayed in the **Desktop Surveillance Serial Keys Management** window header:

- **Subscription end date:** The subscription end date is taken from the serial key with the longest subscription end date.
- **The number of workstation licenses used out of total number:** The number of workstation licenses is summed up from all activated serial keys.
- **The number of server licenses used out of total number:** The number of server licenses is summed up from all activated serial keys.
- **The number of not licensed Clients:** Displays the number of installed Clients with no licenses assigned.

The following information is displayed in the **Desktop Surveillance Serial Keys Management** serial key table:

- Serial key
- Activation date
- Deactivation date (for deactivated keys only)
- Number of workstation licenses
- Number of server licenses
- Key state: activated/deactivated/ expired. For a trial serial key, an expiration date is displayed near the key state.

Deactivating Serial Keys

If for some reason you've decided to discontinue using Desktop Surveillance, you can deactivate serial keys.

To deactivate a serial key, do the following:

1. Make sure you have an active Internet connection on the computer with installed Desktop Surveillance Server.
2. Start the Desktop Surveillance Administrative Panel and select the **Desktop Surveillance** node.
3. Select **Action > Manage Serial Keys,** or right-click the **Desktop Surveillance** node and select **Manage Serial Keys**.
4. The **Desktop Surveillance Serial Keys Management** window opens.
5. Select a serial key to be deactivated and click **Deactivate**.
   NOTE: Expired serial keys can't be deactivated.
6. In the confirmation message, click **Deactivate**.
7. Click **Yes**, when asked to confirm the deactivation.
8. The progress of serial key deactivation is displayed in the **Desktop Surveillance Serial Key Deactivation** window.
9. If a serial key is successfully deactivated, you will see a confirmation message. Click **Close** in the message.
10. The deactivated serial key is marked as **Deactivated** in the **State** column of the **Desktop Surveillance Serial Keys Management** window.
11. The number of available server and workstation licenses and the subscription end date change.
12. Click **Close** in the **Desktop Surveillance Serial Keys Management** window.

Desktop Surveillance Client License Management

Desktop Surveillance client license management is performed in the Administrative Panel.

You can assign a license to a Client or unassign it manually any time. The license can be assigned to an off-line Client and it will be applied after the Client is on-line. The license can be moved from one Client to another. If the Client is uninstalled, its license becomes free and can be assigned to another Client.

NOTE: When the trial serial key expires, the corresponding number of licenses is automatically unassigned from Clients.

Information about the number of used and free licenses of each type is displayed in the status bar of the Administrative Panel and in the **Desktop Surveillance Serial Keys Management** window.

You can manage either licenses for a single Client, or licenses for multiple clients.

To assign the license to one Client, do the following:

1. Start the **CensorNet Desktop Surveillance Administrative Panel**.
2. Select **Desktop Surveillance Clients** in the navigation pane or details pane.

3. Navigate to the Client, to which the license should be assigned. Right click and select **Add Workstation License (Add Server License)**.
4. The license is added to the Client and it starts session monitoring.

To unassign the Client license, do the following:

1. Start the **CensorNet Desktop Surveillance Administrative Panel**.
2. Select **Desktop Surveillance Clients** in the navigation pane or details pane.
3. Navigate to the Client, from which the license should be unassigned. Right click and select **Remove License**.
4. The license is removed the Client and it stops session monitoring.

NOTE: To change the Client license type you don't need to unassign the current license. This will be done automatically.

To manage licenses on several Clients, do the following:

1. Start the **CensorNet Desktop Surveillance Administrative Panel**.
2. Select **Desktop Surveillance Clients** in the navigation pane or details pane.
3. Right click and select **Manage Licenses**.
4. The **Desktop Surveillance Clients Licensing Wizard** opens.
5. In the Workstation Licenses list, select the hosts to which the workstation license will be added. Check the corresponding check boxes. To select all hosts, click **Check All**. To clear selection for all hosts, click **Uncheck All**.
6. In the Terminal Server Licenses list, select the hosts to which the server license will be added. Check the corresponding check boxes. To select all hosts, click **Check All**. To clear selection for all hosts, click **Uncheck All**.

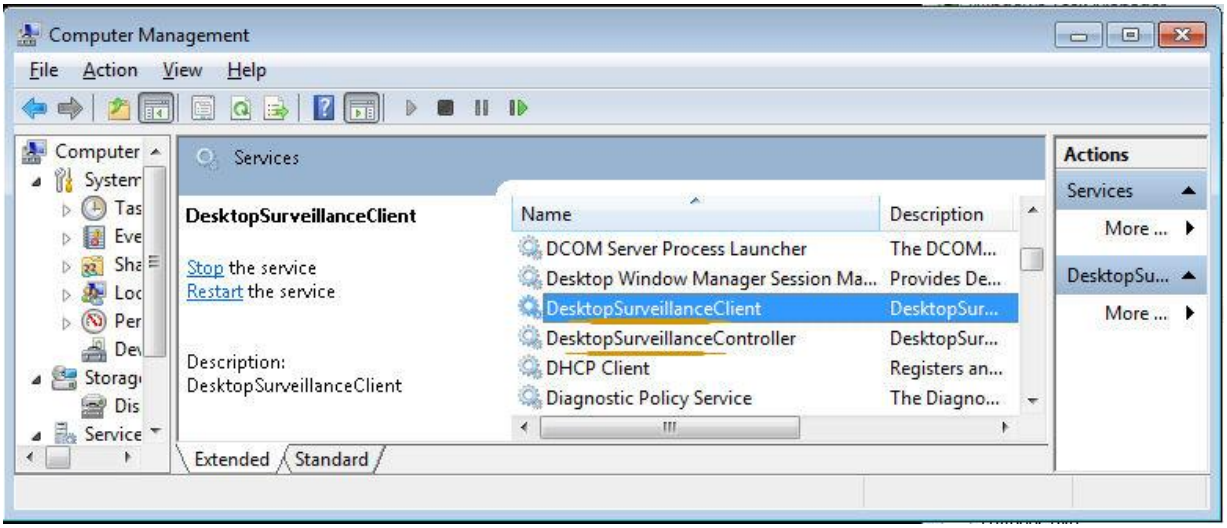
   NOTE: A client can't be selected in both lists. Licenses from all hosts not selected in any list will be removed.
5. Click **Next**. The process of licenses adding/removing starts. When the process finishes, click **Finish**.

Troubleshooting

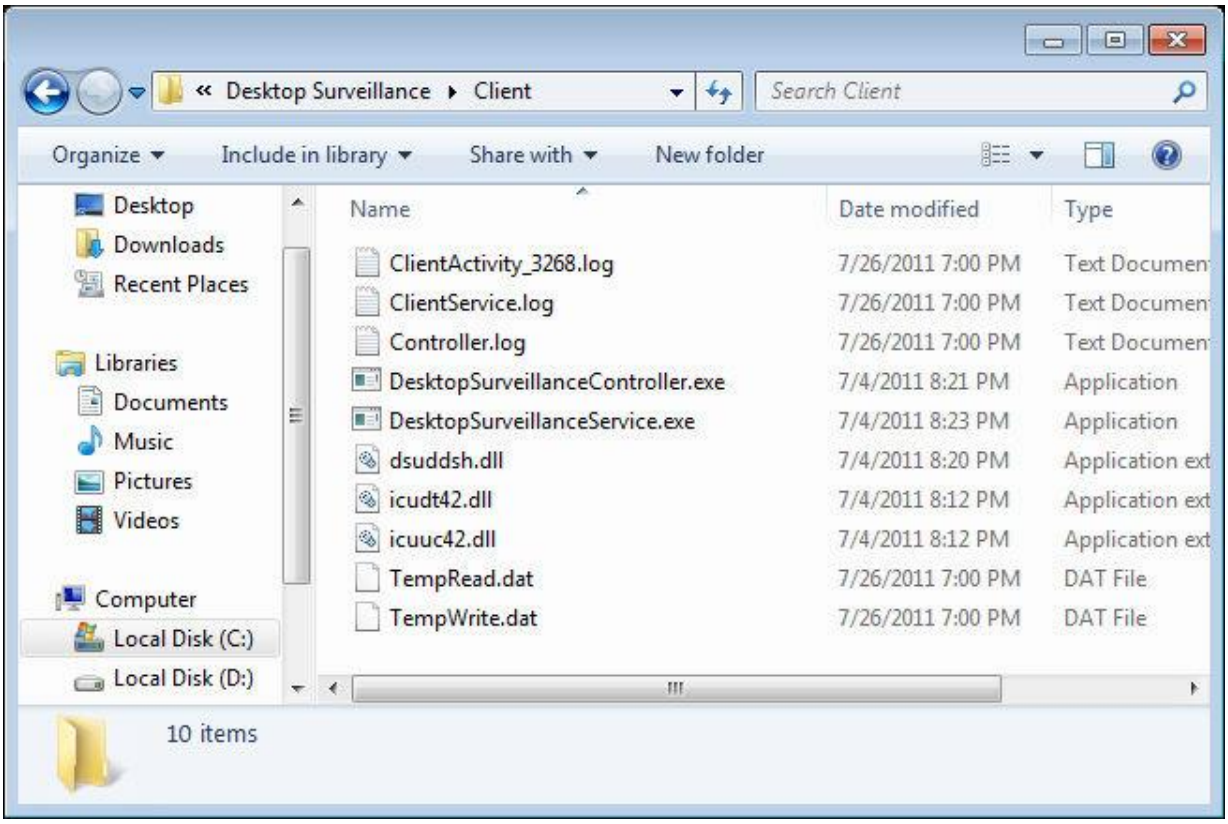
Checking that the Client is Installed

You can check if the Desktop Surveillance Client is installed on the investigated computer in one of the following ways:

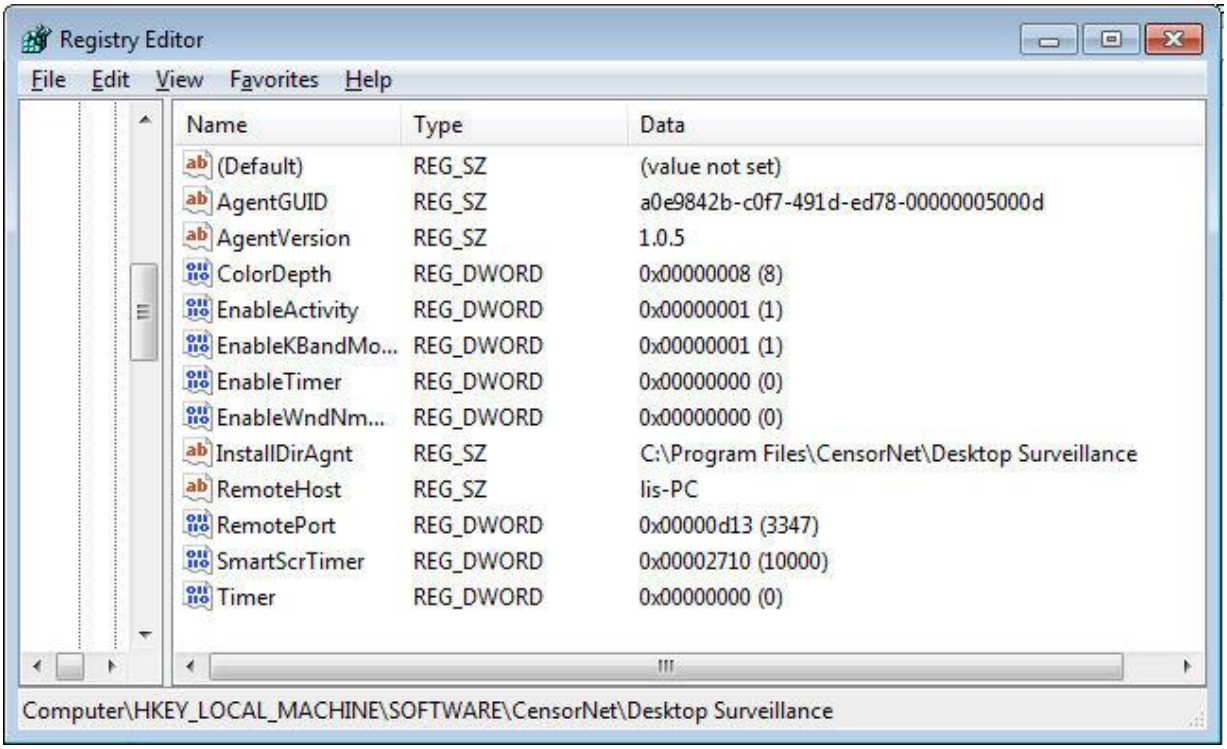
- Two **DesktopSurveillanceService.exe** processes are started on computers with x86 architecture; Two **DesktopSurveillanceService.exe** processes and one **DesktopSurveillanceServicex86.exe** process are started on computers with x64 architecture
- The **DesktopSurveillanceClient** and **DesktopSurveillanceController** services are present;



- There is a **<system disk>:\Program Files\CensorNet\Desktop Surveillance\Client** folder with executable files;



- The **HKEY_LOCAL_MACHINE\SOFTWARE\CensorNet\Desktop Surveillance** key has the following values:



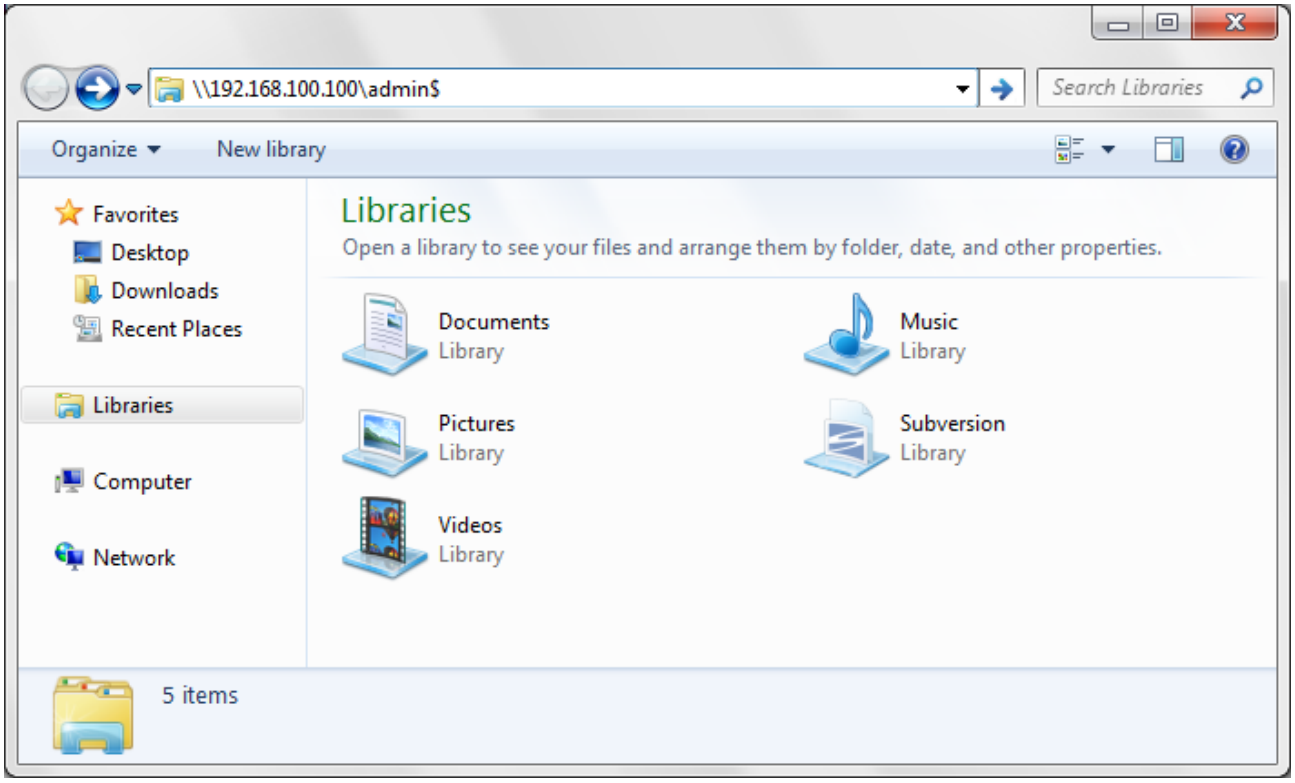
Clients Installation Issues

The common reasons of issues with remote installation or uninstallation of Desktop Surveillance Clients are the inadequate network configuration or system settings.

For successful remote installation, Desktop Surveillance needs to access the administrative shares on the target computers.

To check the administrative shares availability, do the following:

1. Open Windows Explorer.
2. In the address bar type **\\<target_computer_IP>\admin$** and press **Enter**.



3. When the Enter Network Password window opens, enter Administrator credentials and click **OK**.
4. If the login credentials are accepted, the system folder opens (by default, C:\Windows).

If you get an error after performing step 2, try the following:

- Open the Command Prompt (cmd.exe). Enter and execute the **ping <target_computer_name or IP>** command. Check the following:

  1. If you do not get ping replies, network may be down. Check the network connection and try again.
  2. If the network is up, but you don't get the ping reply, check the firewall on the remote computer. Disable the firewall on the target remote computer.

- If you are receiving ping replies, but the administrative share is still unavailable, check that the Sharing Wizard or the Simple file sharing are disabled.
- If you are receiving ping replies and the sharing options are good, but you still cannot access the administrative shares, check that the Server system service is running on the remote computer.
- If none of the mentioned helps to solve the problem, contact your System Administrator.

If you get a login error after performing step 3, try the following:

- Make sure that the credentials you enter are correct. You have to enter the credentials of a Domain Administrator or a local Administrator account on the remote computer.
- Verify that the account password is not empty. Accounts with empty passwords cannot be used for remote connection.
- Try typing the username as **<domain_name>\<username>** if the remote computer is in a domain, or **<computer_name>\<username>** if the PC belongs to a workgroup.
- If none of the mentioned helps to solve the problem, contact your System Administrator.

DNS

Try using the remote computer's IP address if you cannot access it by the name. DNS service may be unavailable in your network.

UAC

If you access the administrative shares normally on the remote PC running Window Vista or Windows 7, but the Desktop Surveillance Client remote installation fails, make sure the User Account Control is disabled on the remote computer.

Remote Client Installation Issues

If you encounter problems with remote installation of Desktop Surveillance Clients in a workgroup under Windows 7/Vista, try enabling the Local Account Token Filter Policy.

NOTE: This is a known Windows issue that might block remote application installation.

To enable Local Account Token Filter Policy:

1. Open the **Windows Registry Editor**.
2. In the **Registry Editor** window, select the following key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
3. Double-click the LocalAccountTokenFilterPolicy value, or select it and click **Modify** in the right-click menu.
4. In the **Value data** box, type 1, and then click **OK**.
5. Close the **Windows Registry Editor**.
6. Deploy Desktop Surveillance Client.
7. Open the **Windows Registry Editor**.
8. In the **Registry Editor** window, select the following key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
9. Double-click the LocalAccountTokenFilterPolicy value or select it and click **Modify** in the right-click menu.
10. In the **Value data** box, type 0, and then click **OK**.

If the LocalAccountTokenFilterPolicy registry value does not exist, follow these steps:

1. In the **Windows Registry Editor** in the **Edit** menu, click **New**, and then click **DWORD Value**.
2. Type LocalAccountTokenFilterPolicy and then press ENTER.

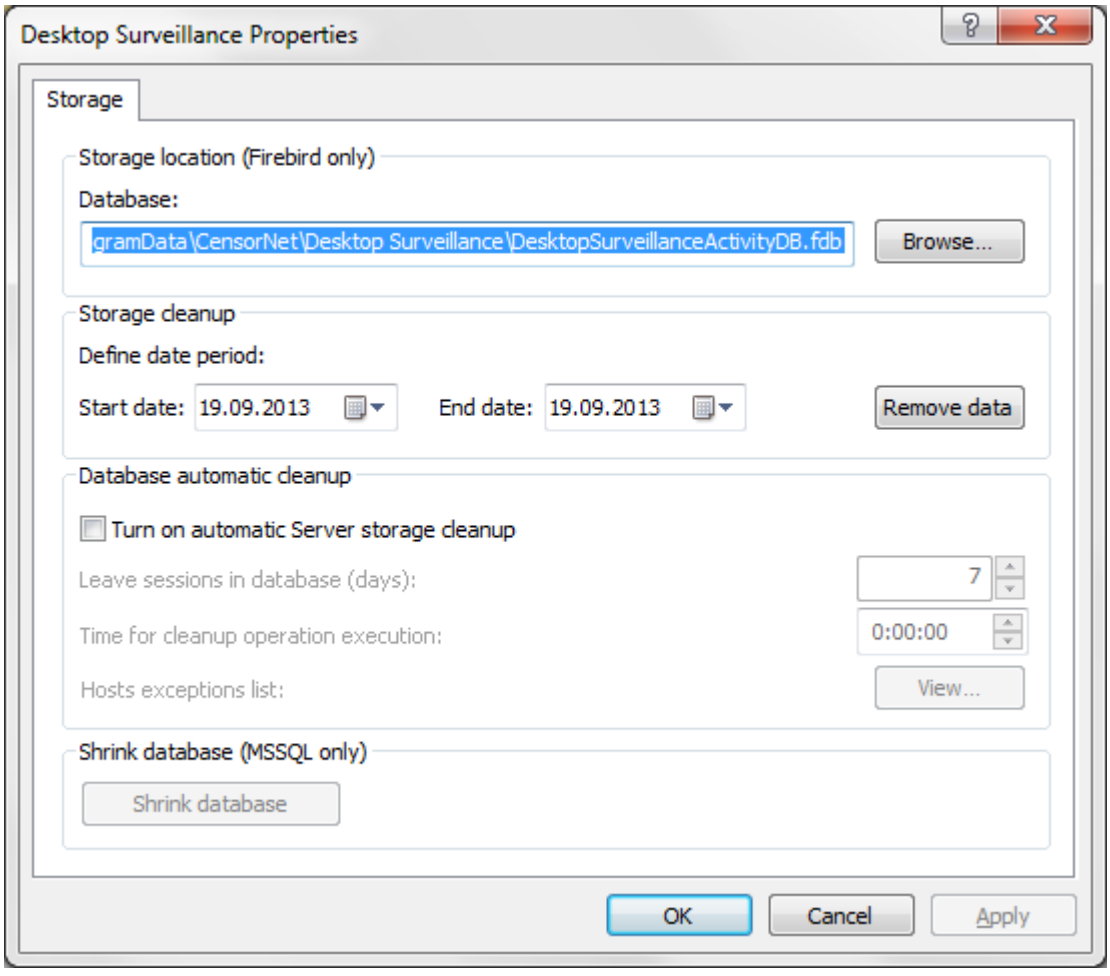
Administrative Panel

Administrative Panel Properties

CensorNet Desktop Surveillance Administrative Panel properties define main properties of data storage.

To define CensorNet Desktop Surveillance properties:

1. Select **Action > Properties** or right-click on the Desktop Surveillance node and select **Properties**.
2. The **Desktop Surveillance Properties** window opens.



3. Define the following settings:
    - Click **Browse** and navigate to the new storage path for screen captures saving.
    - Select the dates in the **Start date** and **End date** fields and click **Remove data** to delete all screen captures created between the specified dates.
    - Select the **Turn on automatic Server storage cleanup** check box to enable automatic database cleanup.
      Define the following parameters:
        - The period for data to be stored before cleaned up automatically.
        - The time for cleanup operation execution.

- Host exceptions list is used to define the computers with Corporate Security Monitor Clients installed whose data will not be deleted during the automatic Server storage cleanup.

NOTE: The exceptions are not available during manual Server storage cleanup.

4. Click **OK** to accept the changes and close the window.

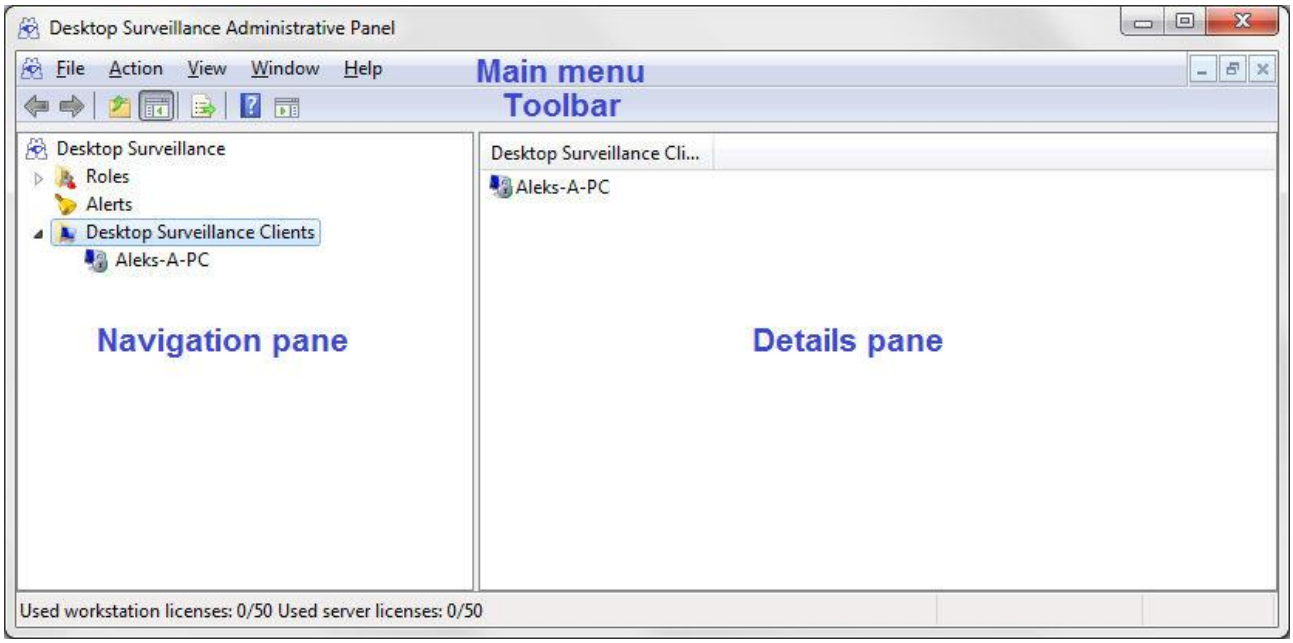
1. **The following properties are available:**
   - **Storage location**: This option defines where created screen captures will be saved and also allows you to move the database to another location. Please make sure that you have enough free space at the selected location.
   - **Storage cleanup:** This option allows you to delete stored data manually or automatically not to run out of disk space.
   - **Database automatic cleanup:** This option allows you to delete stored data from the defined hosts automatically with the defined frequency.

Administrative Panel interface

Administrative Panel Interface

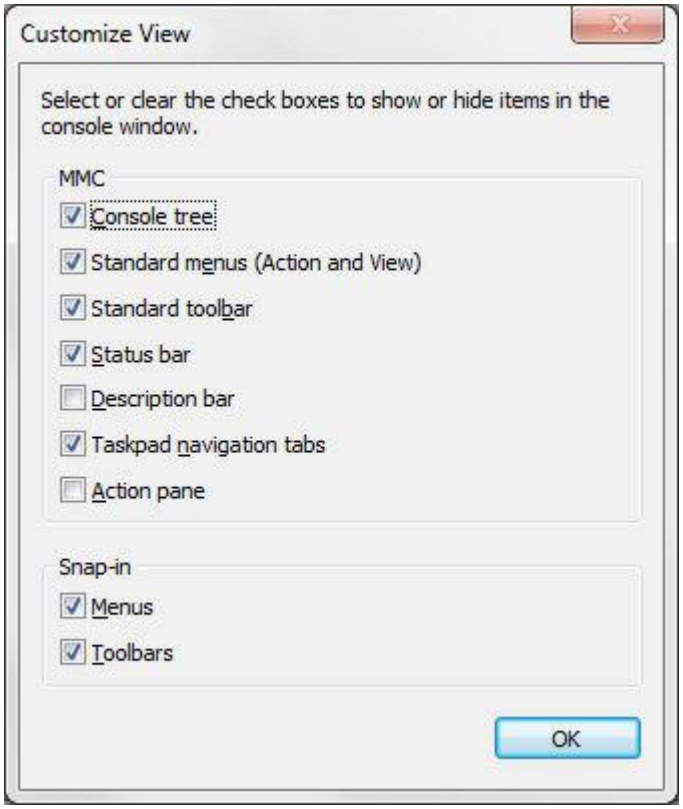
CensorNet Desktop Surveillance Administrative Panel interface includes the following parts:

- **Navigation pane (Console tree)**: This pane includes the tree with one main node **CensorNet Desktop Surveillance** and three main sub-nodes: **Roles**, **Alerts** and **Desktop Surveillance Clients**. The **Roles** node gives you access to the list of users that can use the Desktop Surveillance Viewer. The **Alerts** node allows you to manage the Alerts (notifications about potentially harmful or forbidden actions on the investigated computers). The **Desktop Surveillance Clients** node allows you to manage the **Clients** installed on host computers. The **Navigation** pane can be hidden by selecting **View > Customize** and clearing the **Console tree** box.
- **Details pane:** This pane displays the contents of the node currently selected in the **Navigation** pane for Roles nodes and the Host configuration for Hosts nodes. Data in the **Details pane** can be displayed in one of four standard representations: Large icons, Small icons, List, and Details.
- **Toolbar:** The toolbar allows you to navigate between the objects quickly and adjust program interface. It includes Back, Forward, Up One Level, Show/Hide Console Tree, Export List, and Hide.
- **Main menu**: It includes four menus: File, Action, View, Window, and Help.



CensorNet Desktop Surveillance interface can be adjusted through the **View** menu. The following commands are available:

- **Add/Remove Columns**: Defines the number of columns displayed in the Details pane.
- **Large icons, Small icons, List**, and **Details**: Data representation in the Details pane.
- **Customize:** Defines interface elements to be visible. You can enable\disable displaying of the Navigation pane (Console tree), Toolbar, Action and View menus, the toolbar, the status bar (in the bottom), the description bar (above the Details pane), etc.



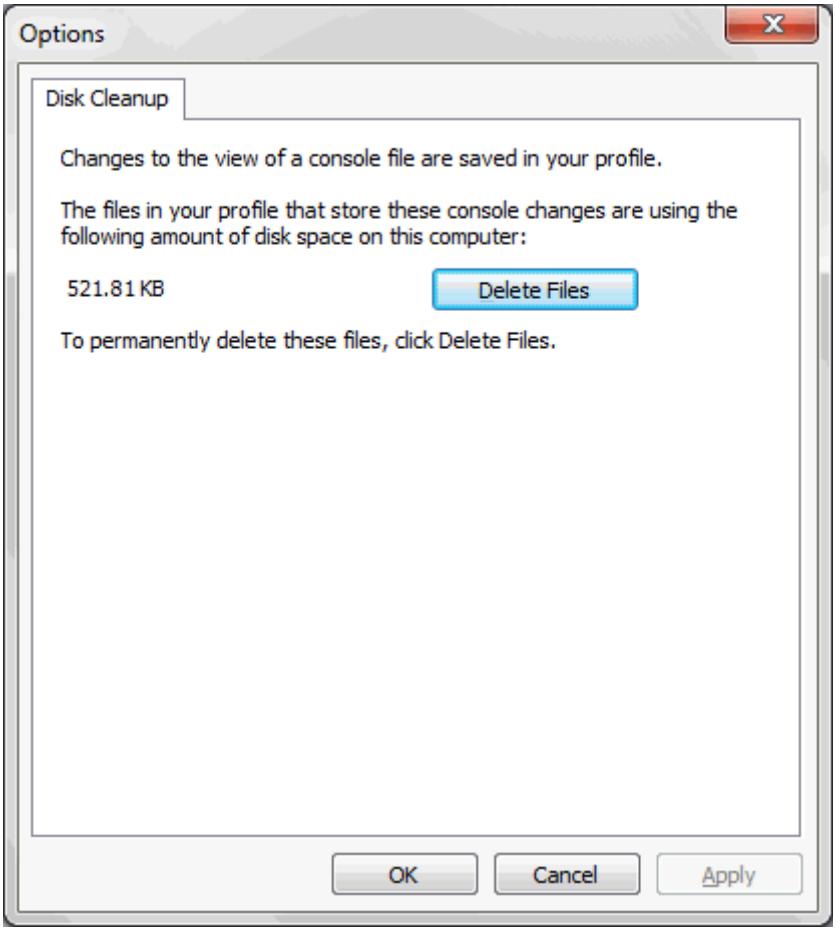
Administrative Panel Options

To get access to options, select **File >Options**.

The Administrative Panel Options allow you to clean the personal settings file records. When you modify the displaying of consoles (for example, by changing the size of a window or adding a new window), MMC saves these settings in a file that preserves your personal settings. The personal settings file records all changes that are made to a console in user mode.

Only the settings that are associated with your profile are deleted. CensorNet Desktop Surveillance Administrative Panel will then display by using the default display settings.

This option is useful if you want to restore the default display settings or if disk space is low.


Options
Disk Cleanup
Changes to the view of a console file are saved in your profile.
The files in your profile that store these console changes are using the following amount of disk space on this computer:
521.81 KB
Delete Files
To permanently delete these files, click Delete Files.
OK
Cancel
Apply

Roles

About Roles

Roles define the sets of Windows users with certain permissions.

Two roles are available in CensorNet Desktop Surveillance:

- **Administrator**: These users are allowed to start both the Desktop Surveillance Administrative Panel and the Desktop Surveillance Viewer.
- **Supervisor**: These users are allowed to start only the CensorNet Desktop Surveillance Viewer.

The roles can be assigned both to users and local groups of the domain and the local computer on which the CensorNet Desktop Surveillance Server and Administrative Panel are installed.

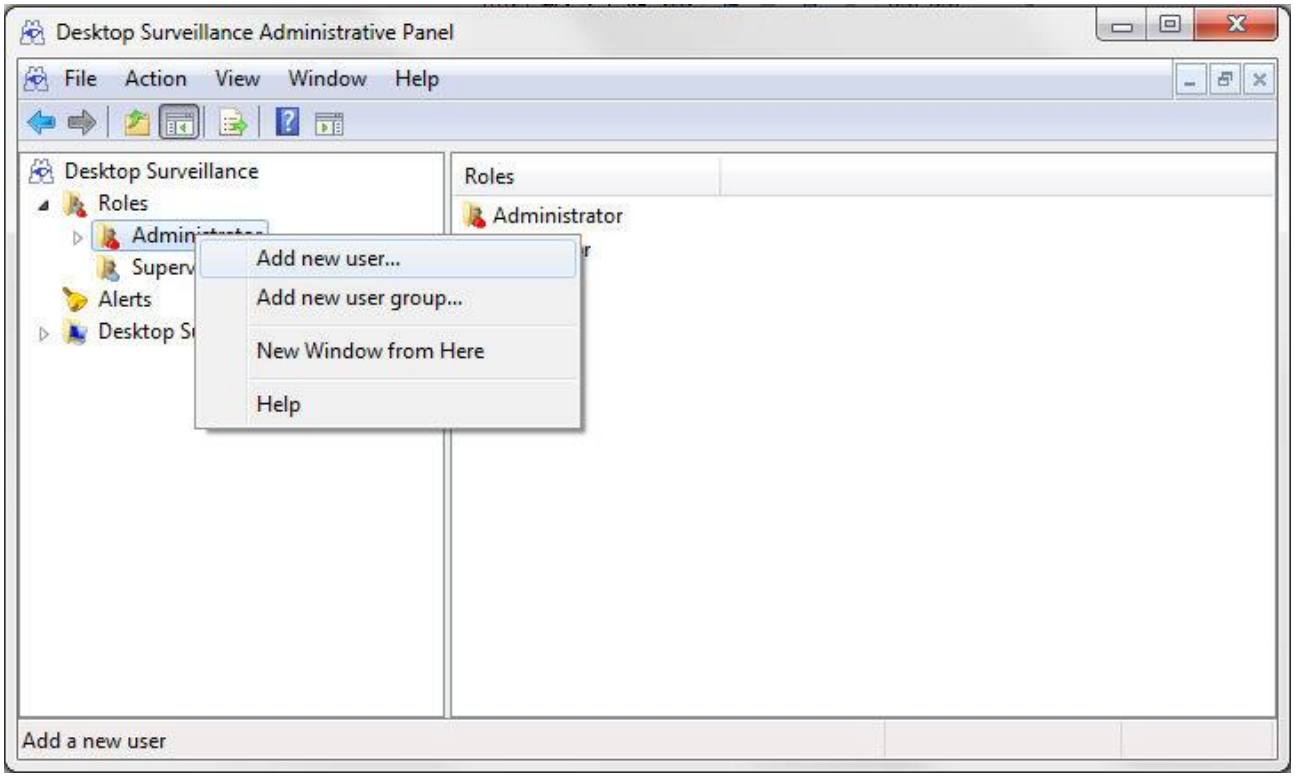
Assigning Roles to Users

There are two ways to assign a role to a user:

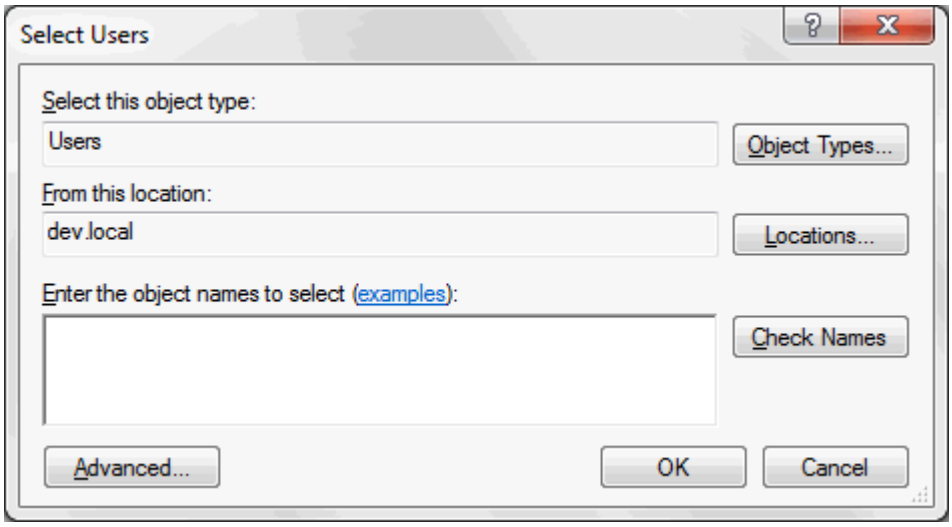
- Enter a user name manually;
- Select a user automatically.

To add a user manually, do the following:

1. Select a role (**Administrator** or **Supervisor**) in the Navigation pane or Details pane.
2. Select **Action > Add new user** or right-click and select **Add new user**.



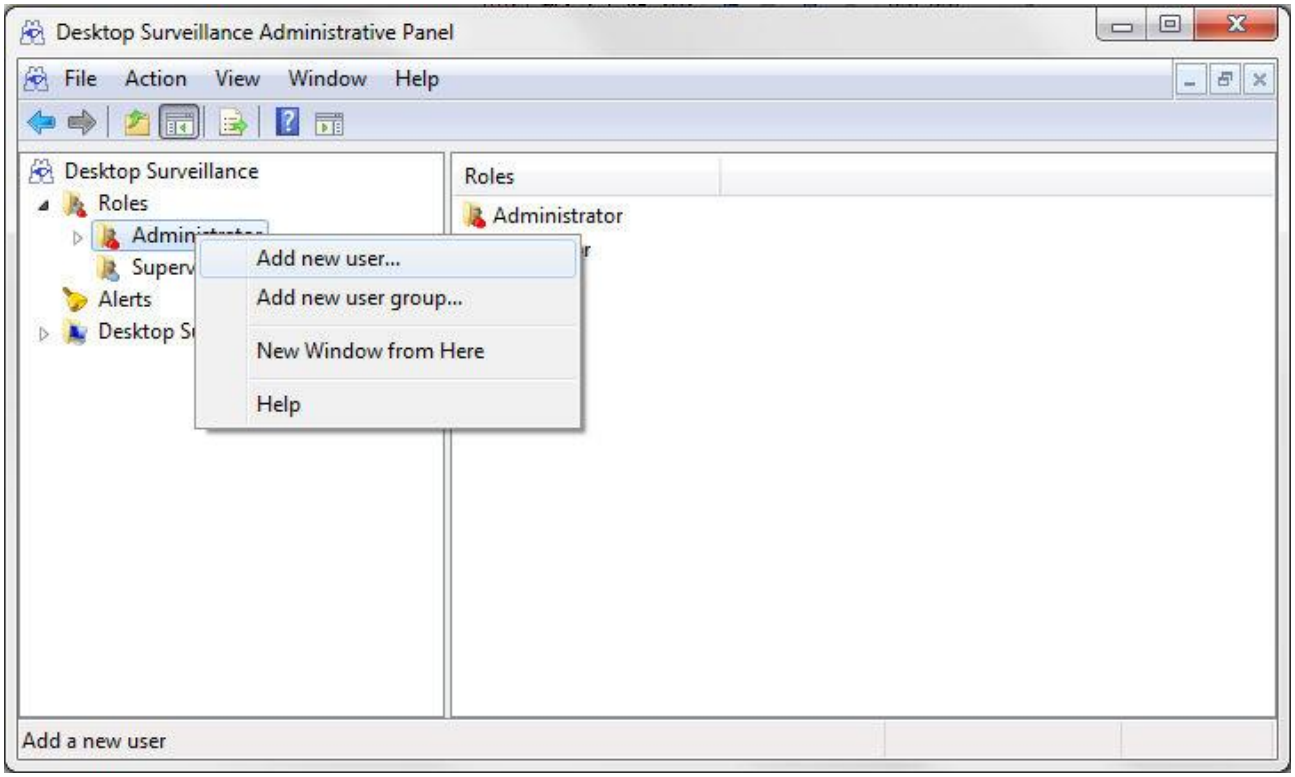
3. The **Select Users** window opens.



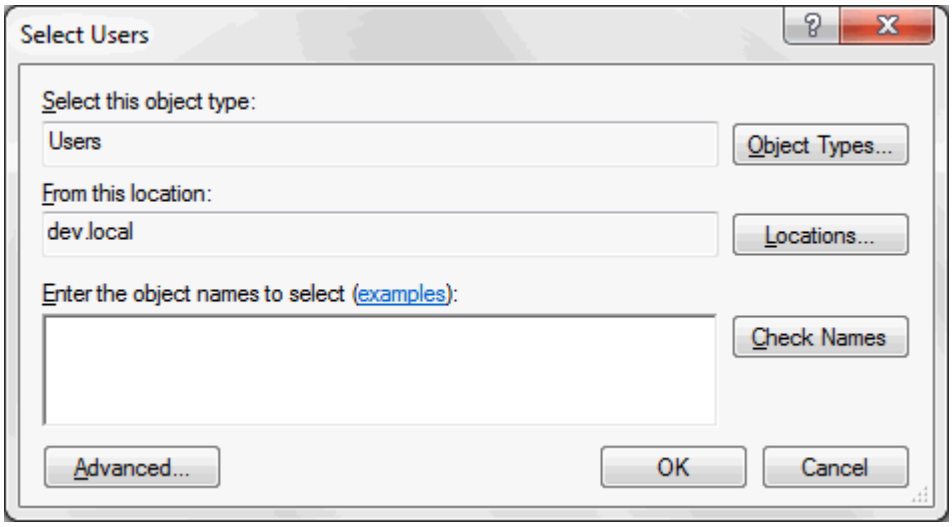
4. Enter the user name in one of the following formats:
    - First Name Last Name (e.g., John Doe)
    - User name (e.g., user_john)
    - User name@Domain name (e.g., user_john@domian1)
    - Domain name\User name (e.g., domain1\user_john)
5. Click **Check Names** to check that the name is entered correctly.
6. Click **OK** to add the user.

To add a user automatically, do the following:

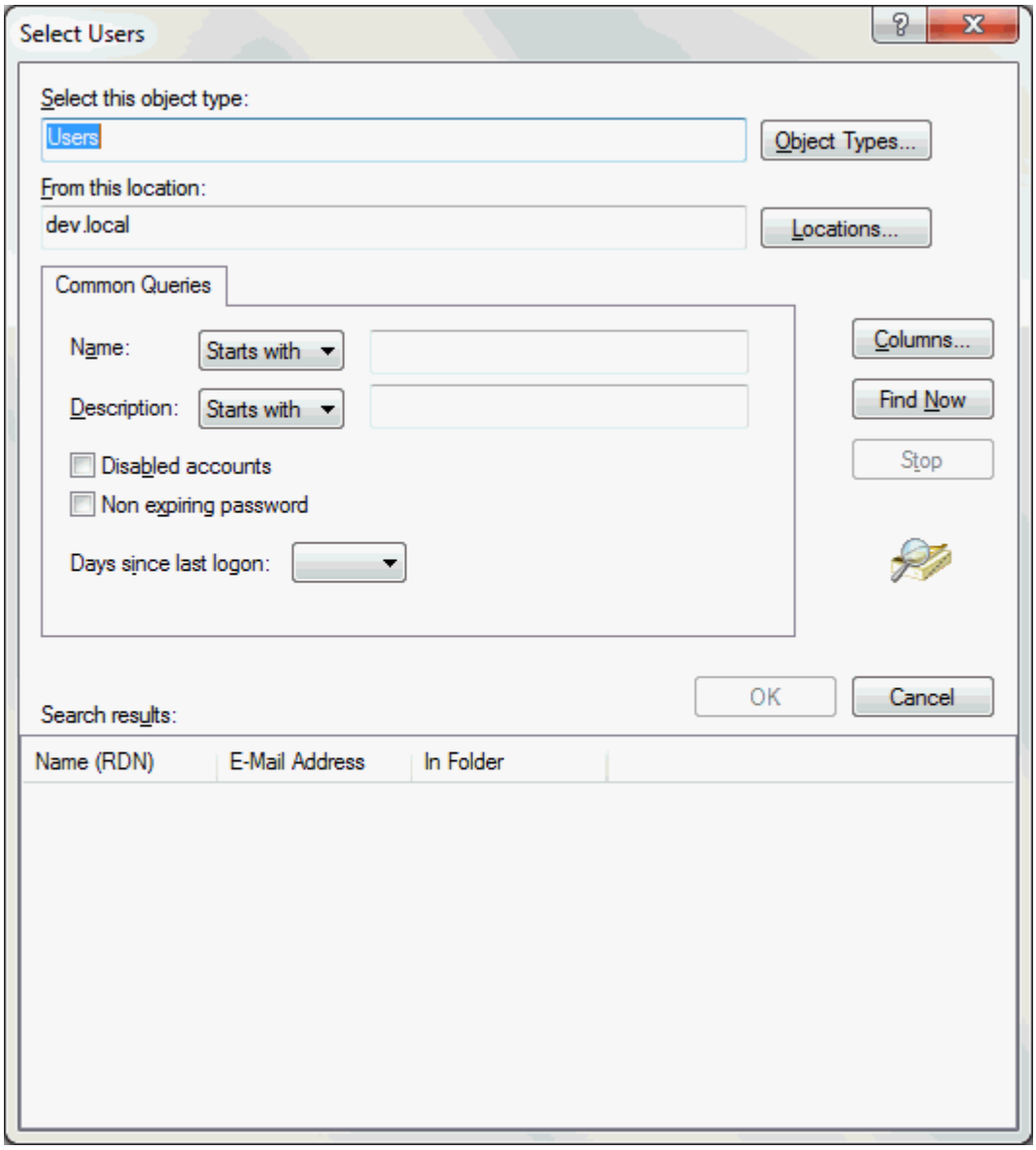
1. Select a role (**Administrator** or **Supervisor**) in the Navigation pane or Details pane.
2. Select **Action > Add new user** or right-click and select **Add new user**.



3. The **Select Users** window opens.



4. Click **Advanced**.
5. The secondary dialog-window opens.



6. Define the query for User search:

- In the **Name** field, define the user name condition. Select the comparison operator from the drop-down list (Starts with or Is exactly). E.g., the User Name starts with "An". This will find users Andrew, Ann, and Angele.
- In the **Description** field, define the user description condition. Select the comparison operator from the drop-down list (Starts with or Is exactly). E.g., the User Description is exactly "John Doe". This will find a user with description John Doe.
- Select the **Disabled accounts** options to select only users with disabled accounts.

7. Click **Find Now** to start search.
8. The users are found and displayed in the list. Select the users to be added to CensorNet Desktop Surveillance and click **OK**.
9. The selected users are displayed in the corresponding field of the main **Select Users** window. Click **OK**.

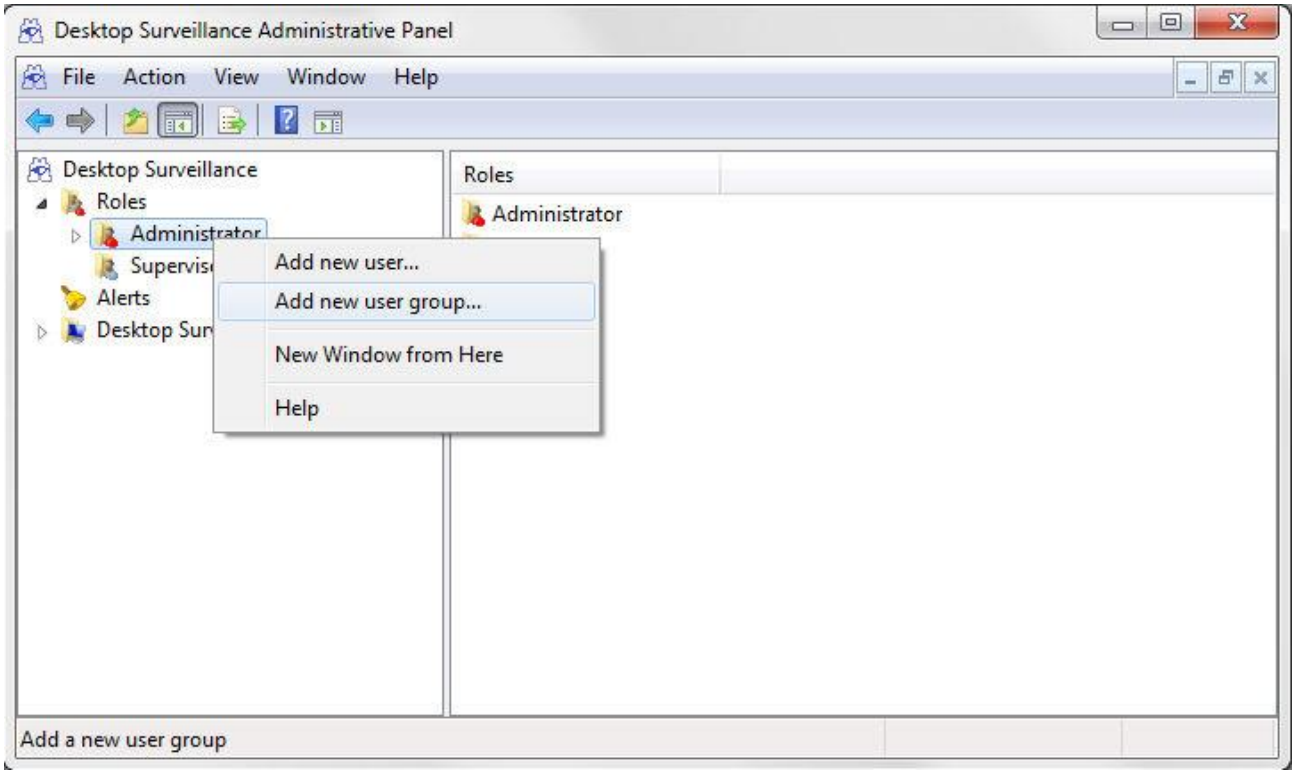
Assigning Roles to User Groups

There are two ways to define a user group:

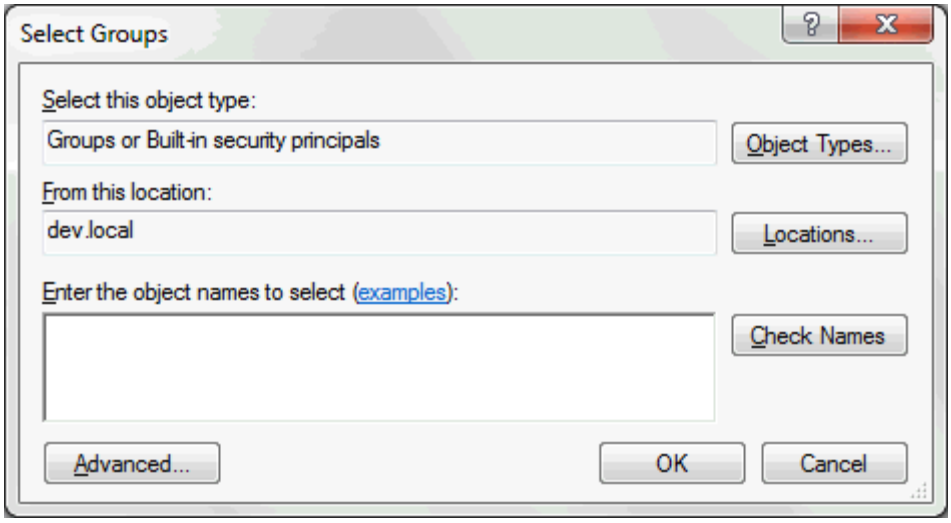
- Enter a user group name manually.
- Select a user group automatically.

To add a user group manually, do the following:

1. Select a role (**Administrator** or **Supervisor**) in the Navigation pane or Details pane.
2. Select **Action > Add new user group** or right-click and select **Add new user group**.



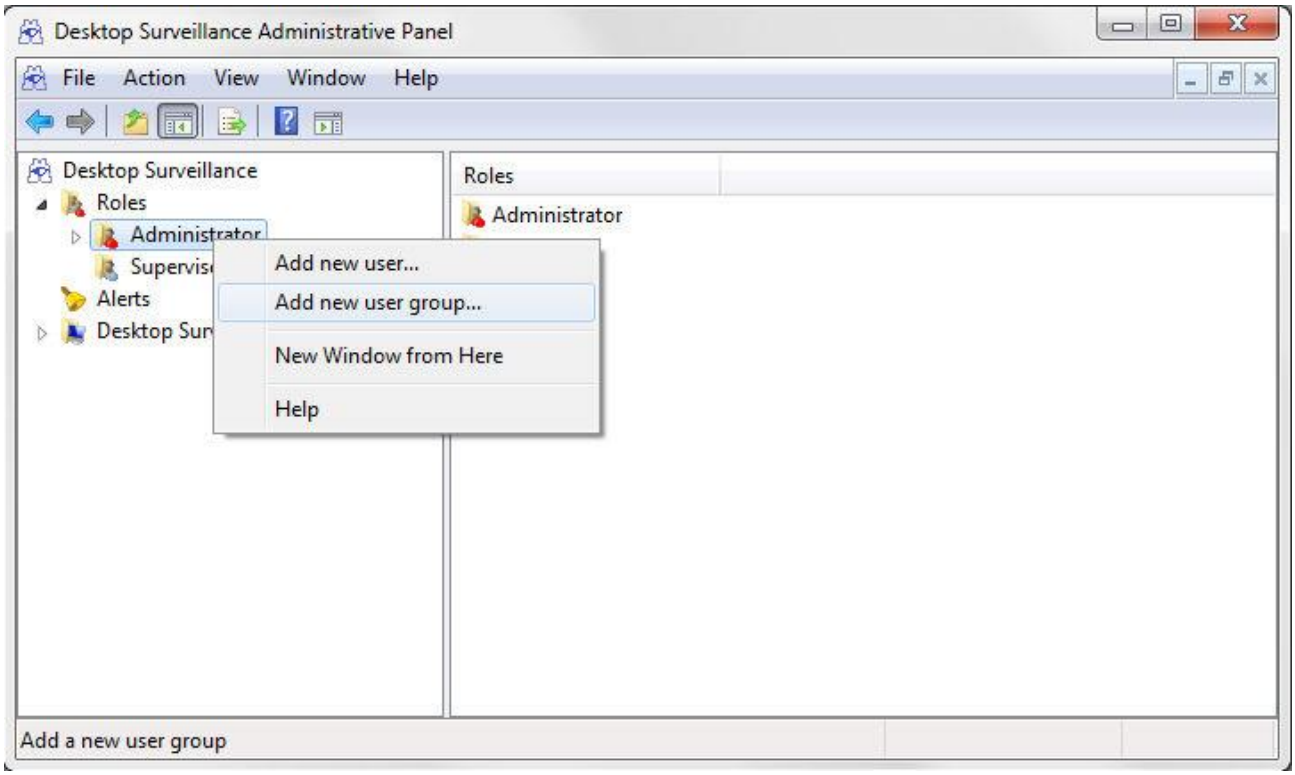
3. The **Select Groups** window opens.



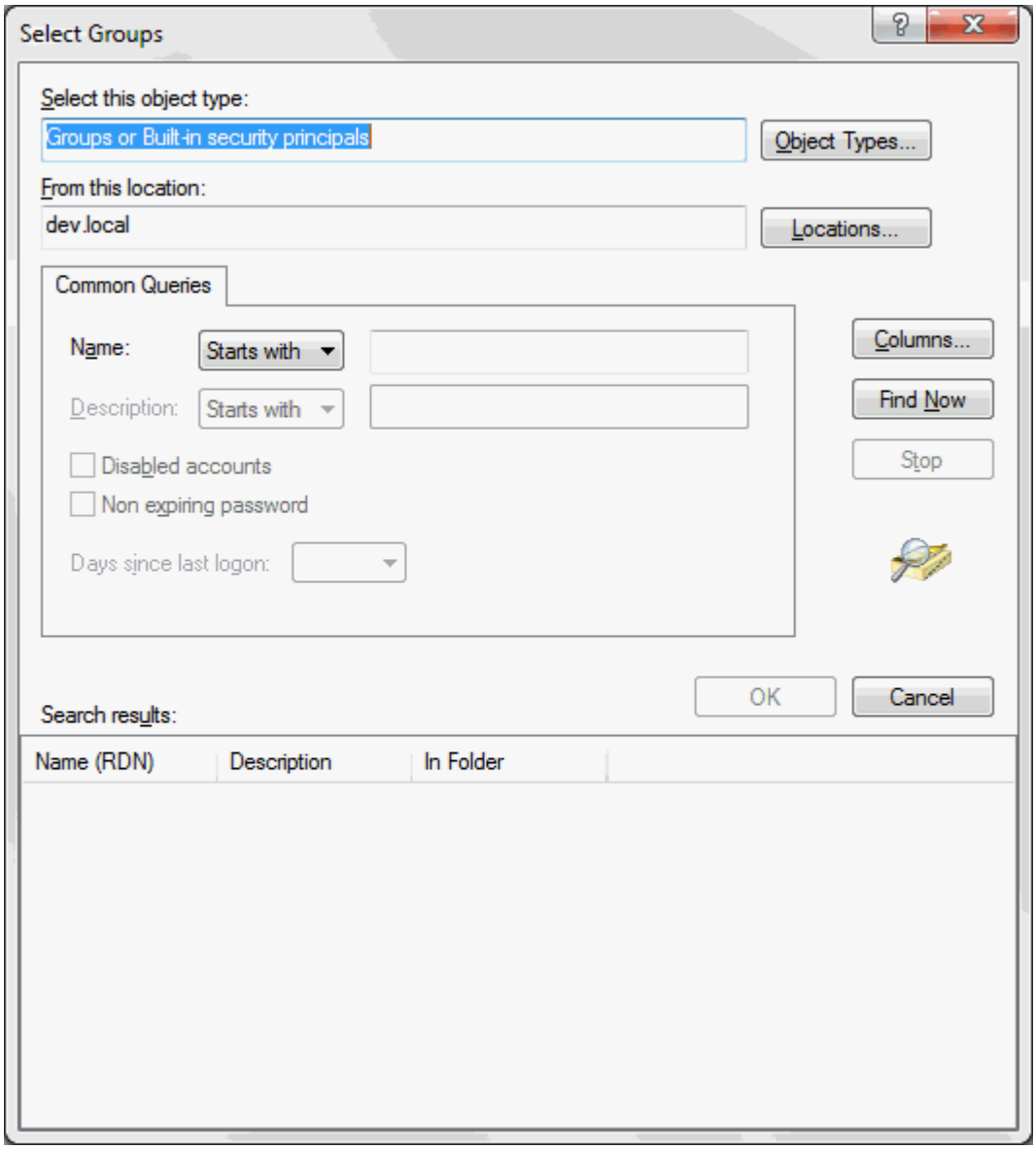
4. Enter the user group name.
5. Click **Check Names** to check that the name is entered correctly.
6. Click **OK** to add the user group.

To add a user automatically, do the following:

1. Right-click on the **Administrator or Supervisor** node in the **CensorNet Desktop Surveillance** tree-view and select **Add new user group** in the context menu.



2. The **Select Groups** window opens.
3. Click on the **Advanced** button.
4. The secondary dialog-window opens.



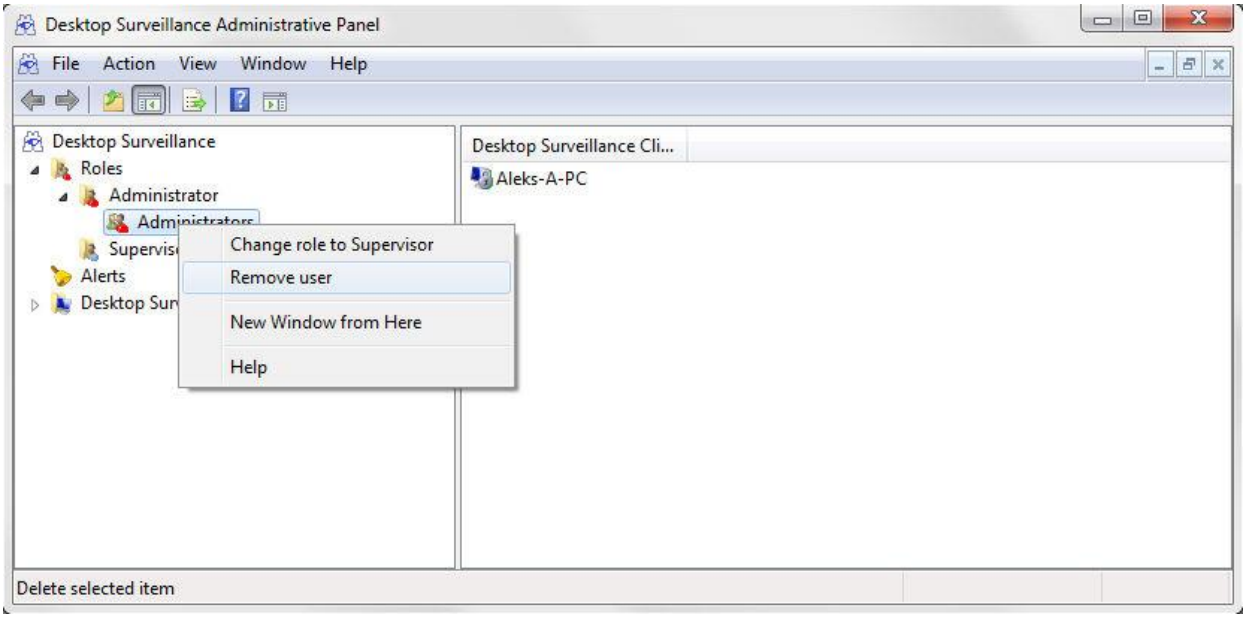
5. Define the query for Groups search:in the **Name** field, define the user name condition. Select the comparison operator from the drop-down list (Starts with or Is exactly). E.g., the User Name starts with "An". This will find users Andrew, Ann, and Angele.
6. Click on the **Find Now** button to start search.
7. The user groups are found and displayed in the list. Select the user groups to be added to CensorNet Desktop Surveillance and click **OK**.
8. The selected user groups are displayed in the corresponding field of the main **Select Groups** window. Click **OK**.

Unassigning Roles from Users/User Groups

To remove a user or a user group role, do one of the following:

1. Select a required user in the **Navigation** pane or **Details** pane.
2. Do one of the following:
   - Right-click and select **Remove user**.

- Select **Action > Remove user**.



3. The selected user or user group are removed from the node and deprived of the respective role.

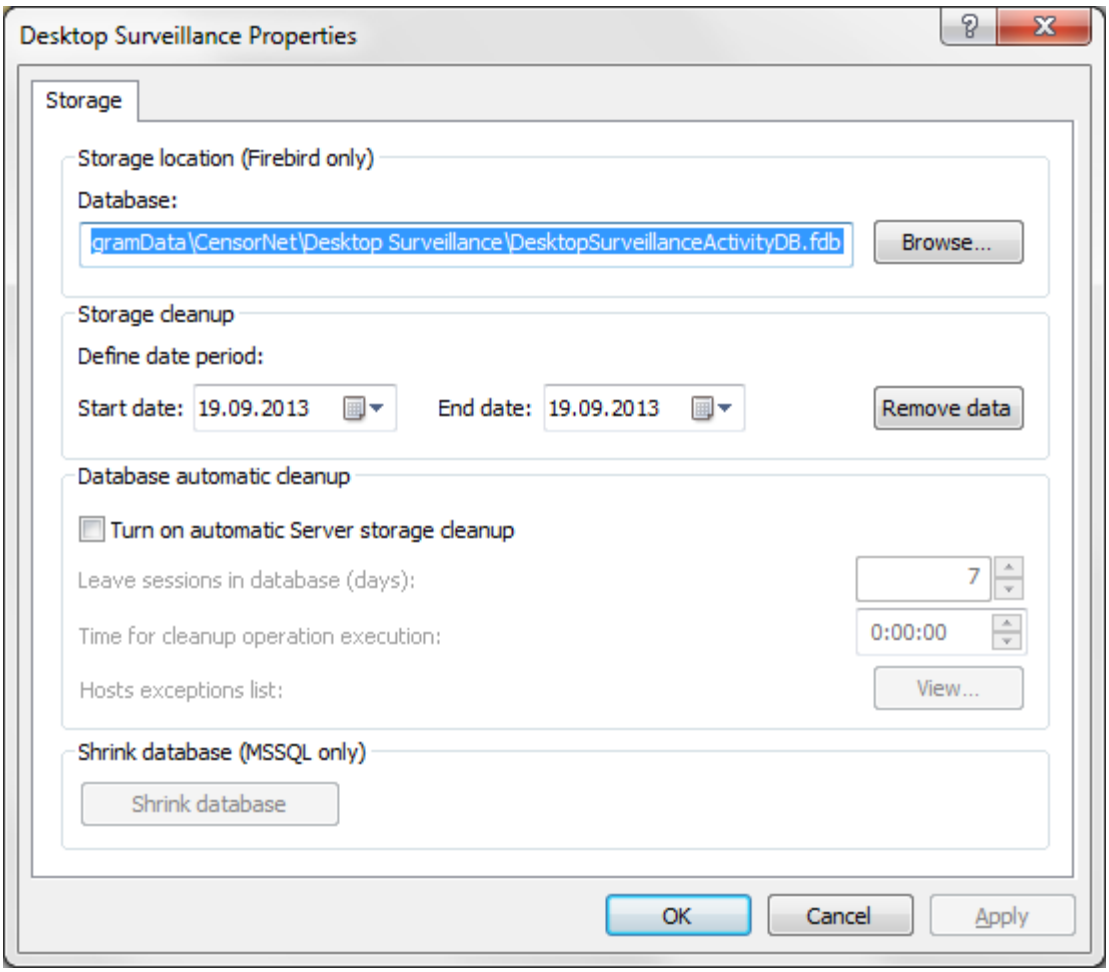
Working with data

Moving Desktop Surveillance Server Database

For some reason, you may need to change the location of the Desktop Surveillance Server database to another disk or directory.

To change the location for Desktop Surveillance Server database:

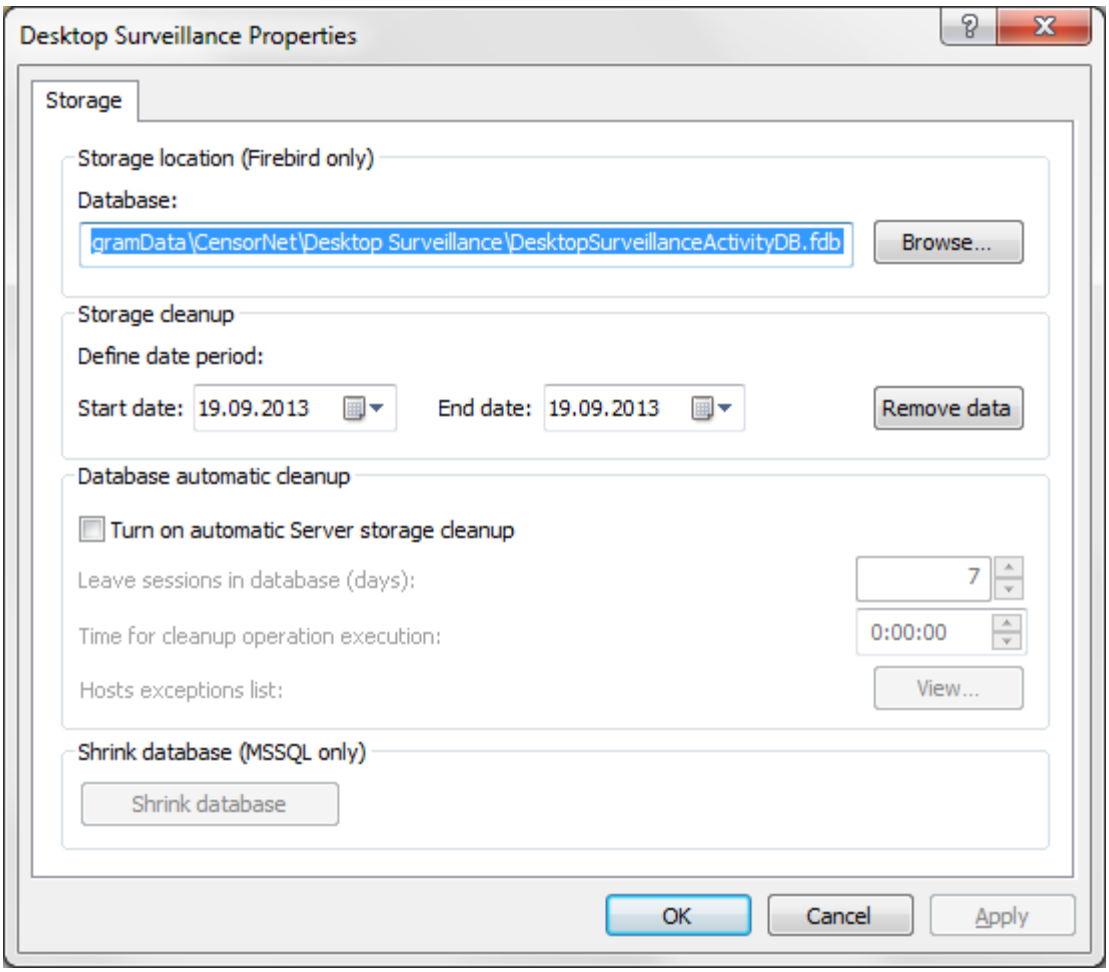
1. Select **Action > Properties** or right-click on the Desktop Surveillance node and select **Properties**.
2. The **Desktop Surveillance Properties** window opens.
3. In the **Storage location** group of options, do one of the following:
    - In the **Path** box, enter the path to the database manually.
    - Click **Browse** and navigate to the destination folder.
4. Click **OK** to accept the changes and close the window.



Deleting Data

To delete data from Desktop Surveillance Server manually:

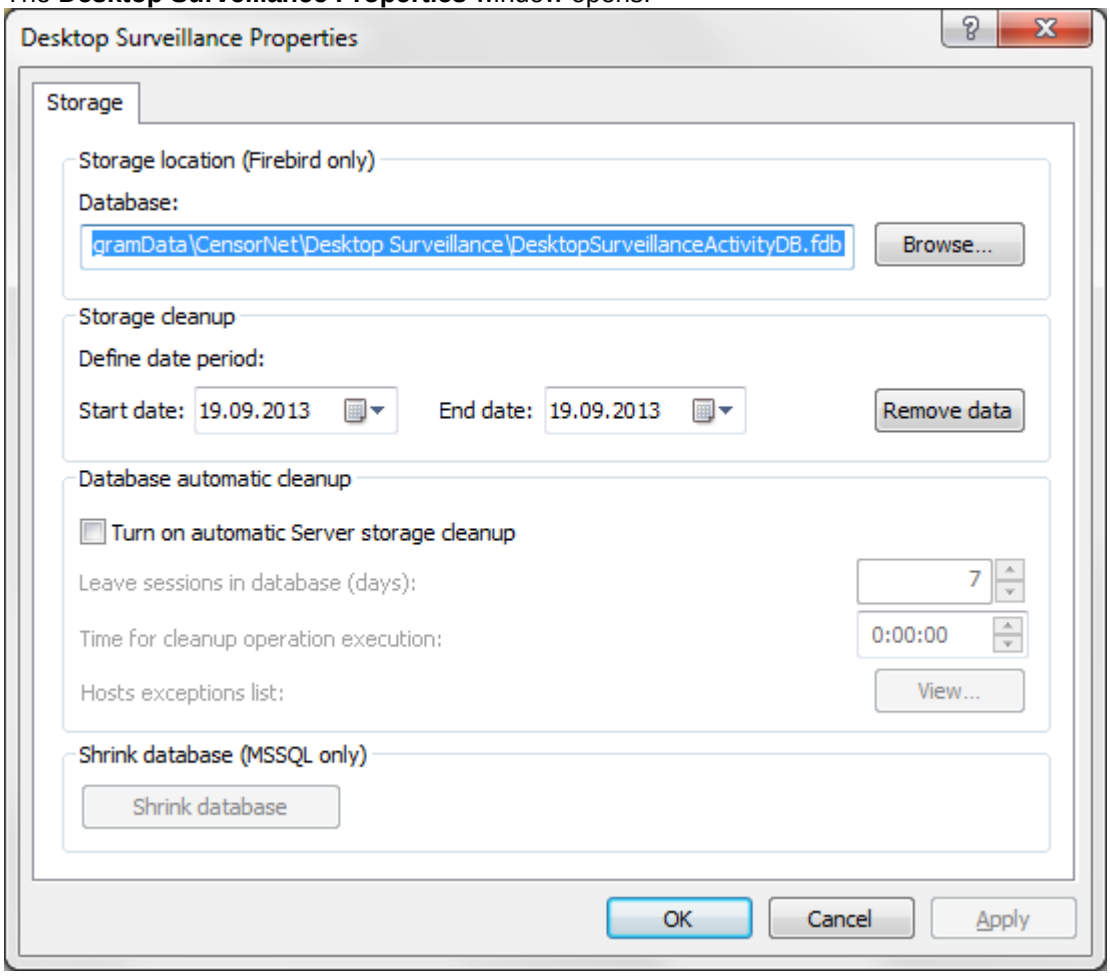
1. Select **Action > Properties** or right-click on the Desktop Surveillance node and select **Properties**.
2. The **Desktop Surveillance Properties** window opens.
3. In the **Database cleanup** group of options, select the date in the **Start date** and **End date** fields and click **Remove data** to delete all screen captures created earlier than the selected date.
4. Click **OK** to accept the changes and close the window.



To delete data from Desktop Surveillance Server automatically:

1. Start the Administrative Panel. Select the **Desktop Surveillance** node.
2. Select **Action > Properties,** or right-click on the Desktop Surveillance node and select **Properties**.

3. The **Desktop Surveillance Properties** window opens.



4. Select the **Turn on automatic Server storage cleanup** check box.
5. Define the number of days to store data before deleting. Define the time to execute the clean-up operation.
6. Click **View** to define the host exceptions. Hosts in the exceptions list will not have their sessions deleted from the database.
7. Click **OK** to accept the changes and close the window.

Automatic database clean-up will be performed with the defined interval at the selected time.

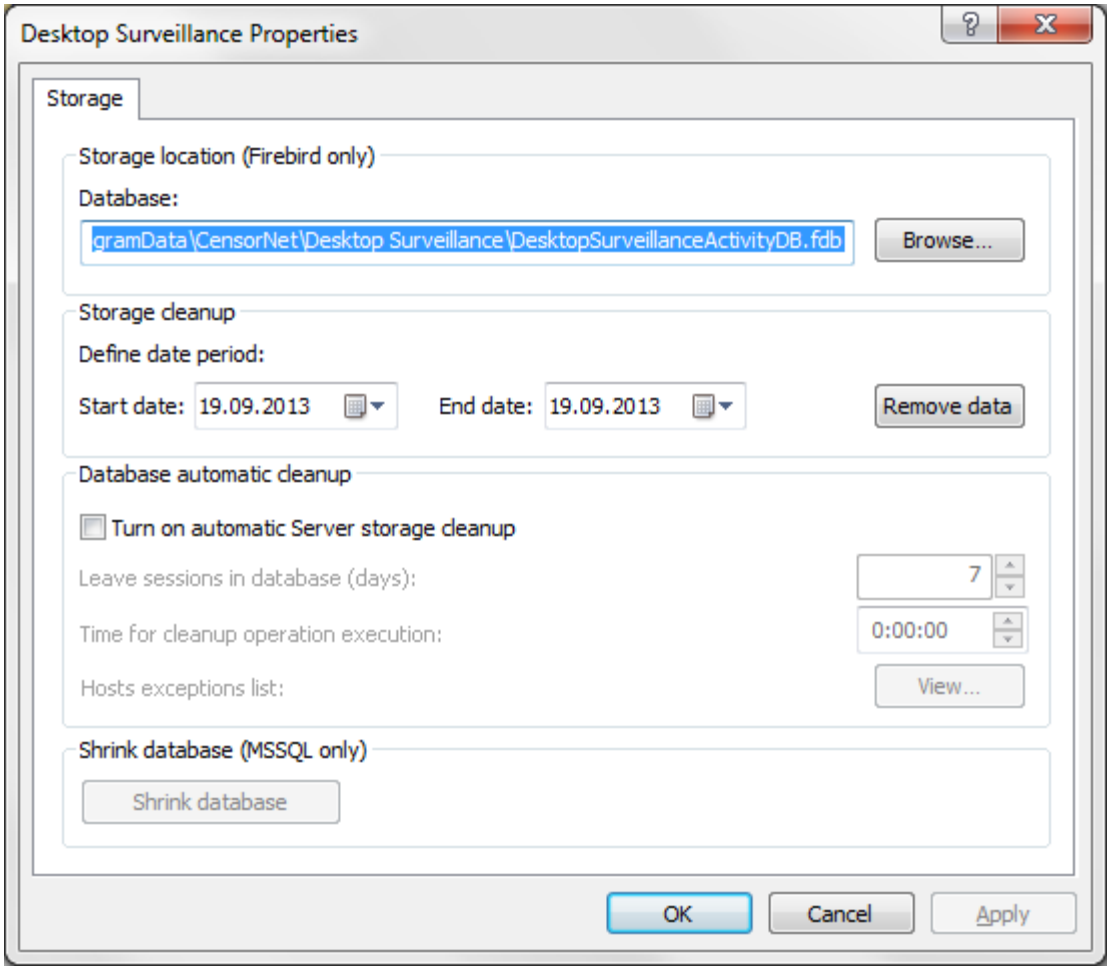
Shrinking Database

The database shrinking feature allows you to shrink the size of the MS SQL database to the actual amount of the data stored in it by cutting the space reserved by the database, but which is not used by it.

NOTE: The database shrinking procedure may take some time (up to several hours) and cause performance slowdown.

To shrink a database, do the following:

1. Start the Administrative Panel. Select the **Desktop Surveillance** node.
2. Select **Action > Properties** or right-click on the **Desktop Surveillance** and select **Properties**.
3. The **Desktop Surveillance Properties** window opens.



4. Click **Shrink database**.

NOTE: The progress of the database shrinking process is not displayed in the Administrative Panel and there is no indication of the process finishing.

Alerts

About Alerts

Alerts are instances that notify the investigator of a specific activity (potentially harmful/forbidden actions) on the target computers on which Clients are installed and allow the investigator to respond to such activity quickly without performing searches.

The notifications can be received in email or tray. Besides screen captures generated on alert events are marked as Alert in the Viewer.

Alert system can be used for two purposes:

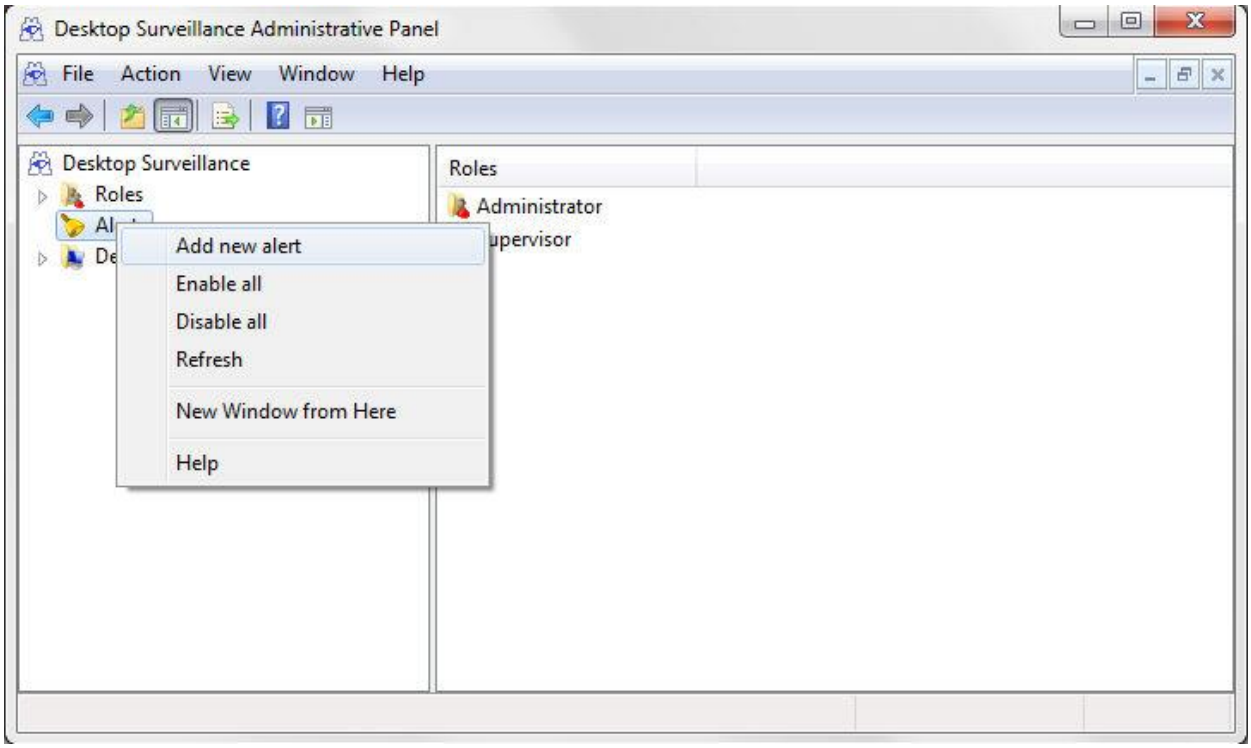
- **Immediate response**: This allows the investigator to get immediate information about the forbidden action and respond to it quickly (almost at once).
- **Delayed response**: This allows the investigator to get information on batch of forbidden actions on multiple clients, analyze them and then respond.

Alerts management

Adding Alerts

To add an alert, do the following:

1. Right-click the **Alerts node** and select **Add New Alert**.

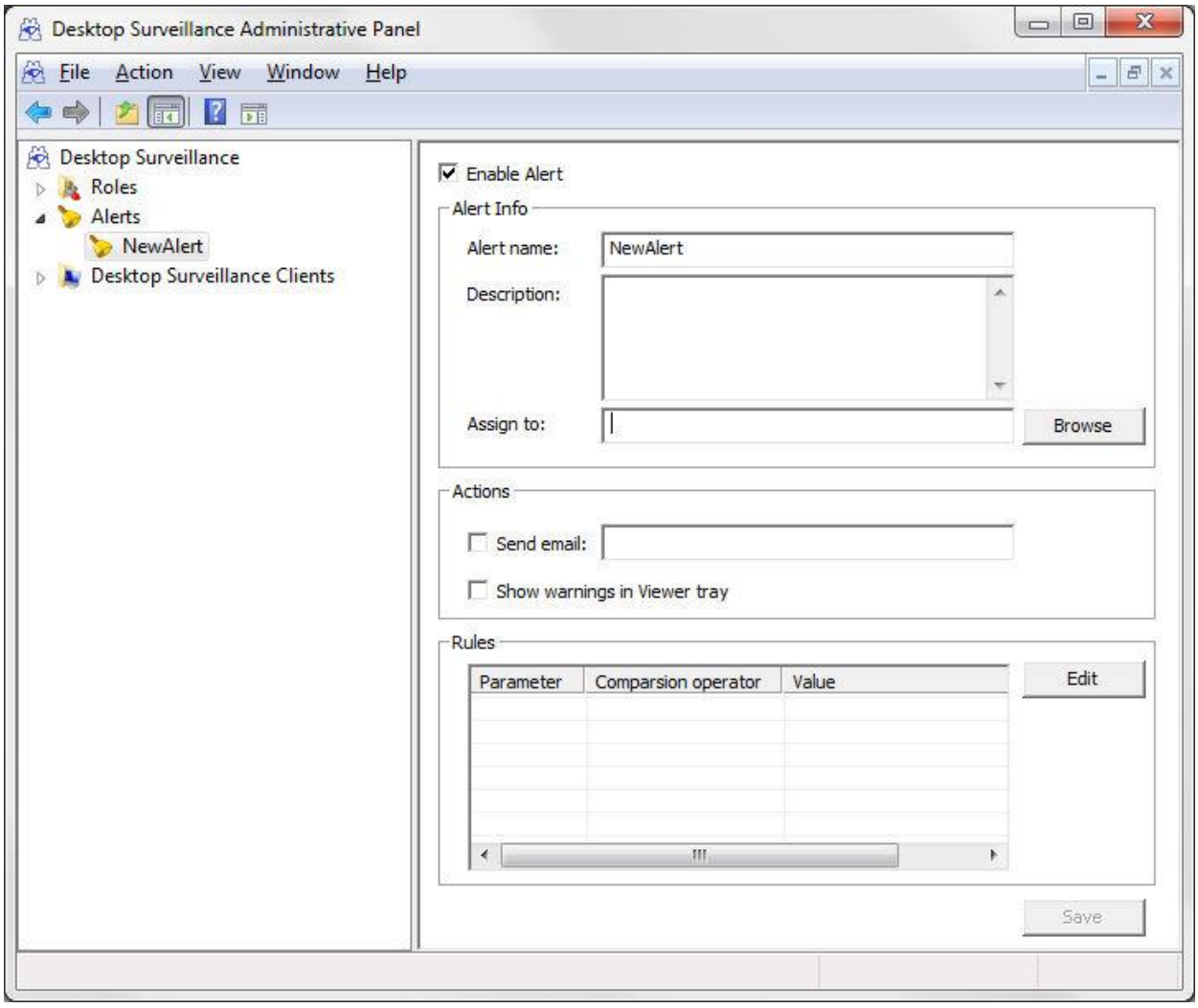


2. A new alert sub-node appears in the tree-view.
3. The Alert editing area for the new alert opens to the right.
4. Enter a unique alert name and alert description (optional).
5. Click **Browse** and select hosts to which the Alert will be assigned.
6. Define alert parameters,
7. Define at least one rule.
8. Click **Save** to save the created Alert.
9. The Alert appears in the tree-view.

Editing Alerts

To edit an alert, do the following:

1. Left-click an alert sub-node in the tree-view.
2. The **Alert editing area** for the new alert opens to the right.

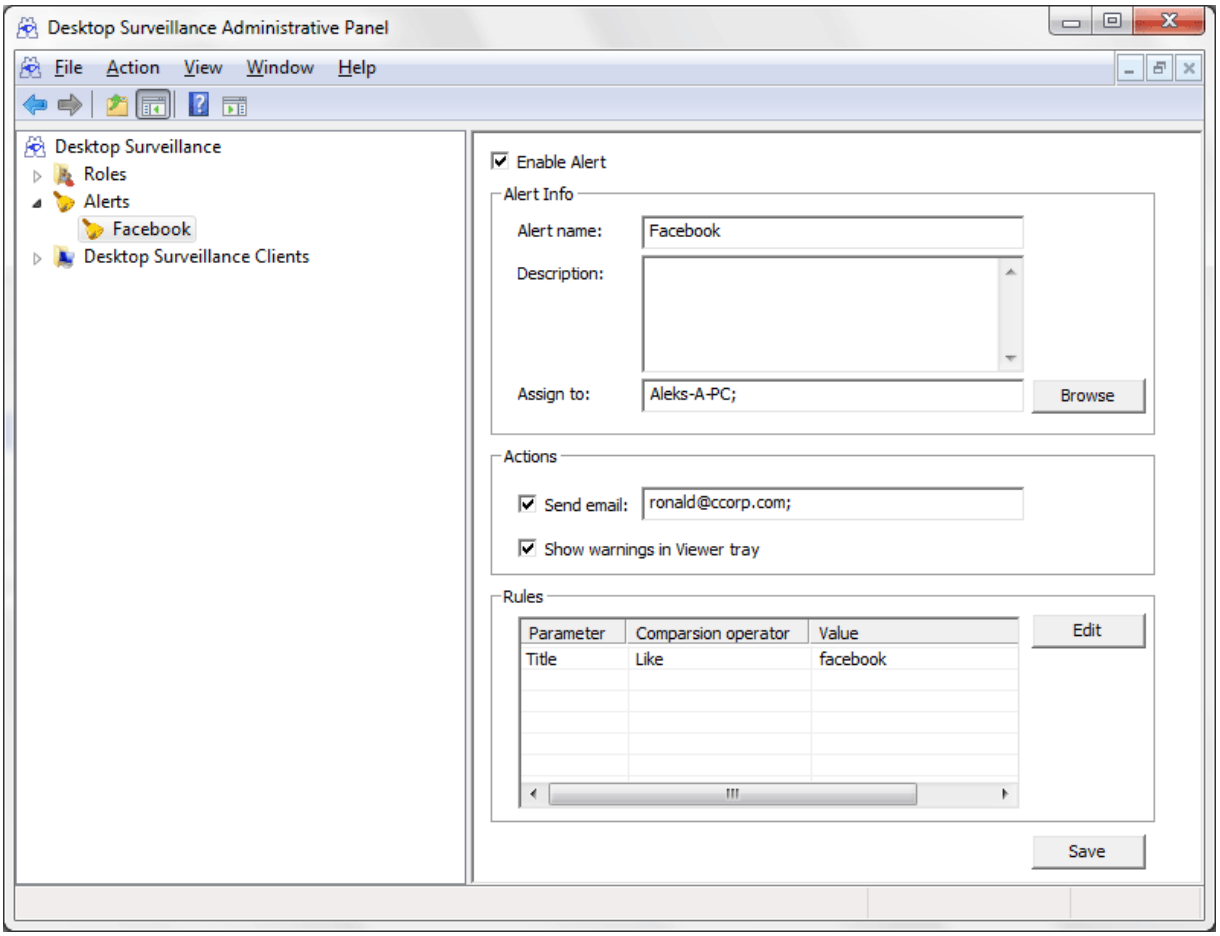


3. Edit the parameters you need.
4. Click **Save** button.
5. The edited parameters are saved.

Viewing Alerts

Alerts are displayed in the tree-view pane to the left. The Alerts node is displayed in the tree-view between the Roles and the Desktop Surveillance Clients nodes. Alerts are displayed as sub-nodes of the Alert node. Each alert sub-node is named with a unique Alert name.

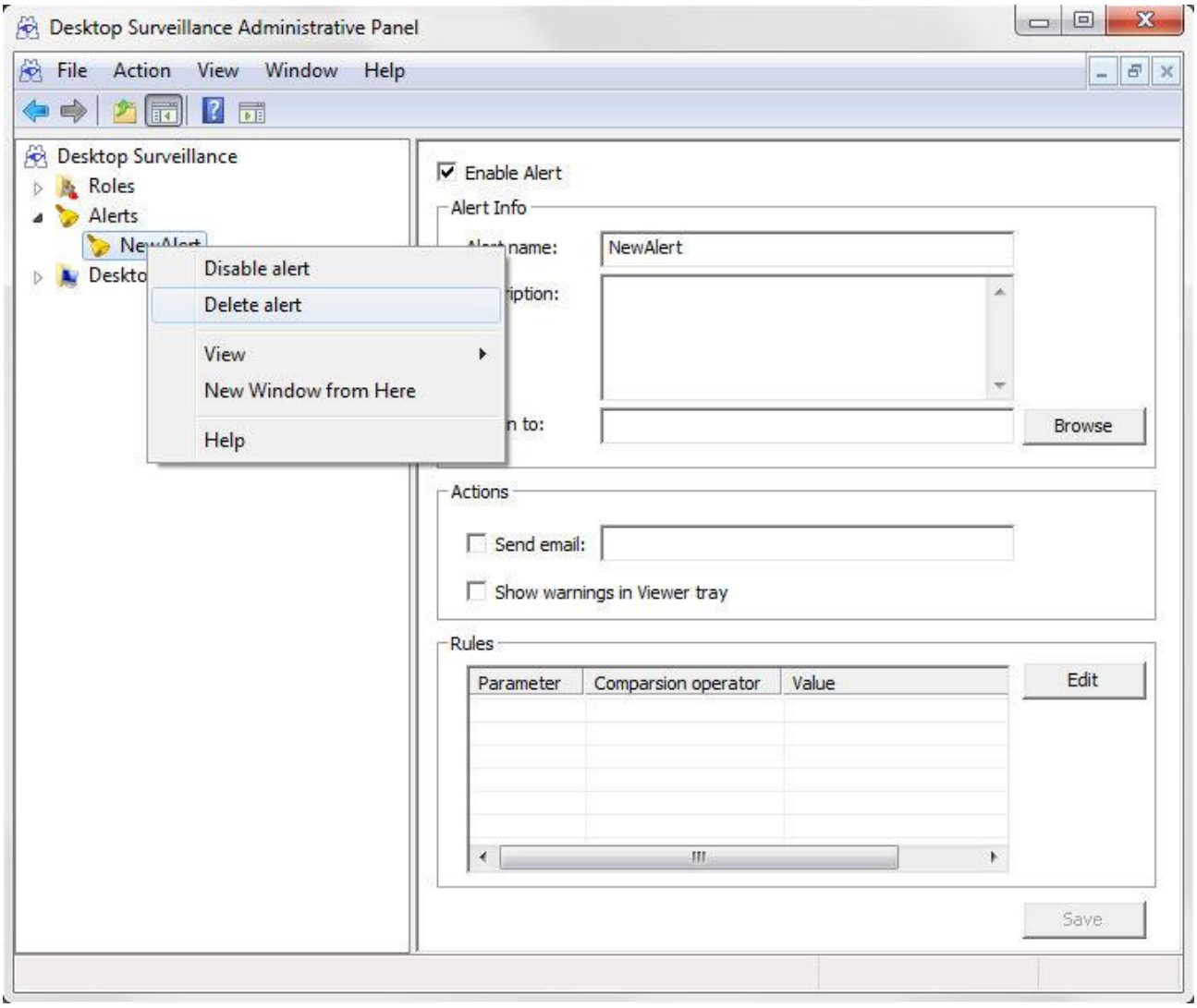
When an alert node is selected, its parameters are displayed in the pane to the right and can be edited.



Deleting Alerts

To delete an alert, do the following:

1. Right-click an alert sub-node in the tree-view and select **Delete Alert**.



2. The confirmation message appears.
3. Click **Yes**.
4. The alert is deleted.

Alert Parameters

The **Alert editing pane** allows you to define the Alert settings and rules.

To edit the Alert Parameters, do the following:

1. Select the required Alert from the **Alerts** node in the tree-view pane to the left.
2. The **Alert editing pane** opens to the right.
3. Enable/disable the selected Alert by checking/clearing the **Enable Alert** check box. If the Alert is disabled, you will not receive notifications on it (the screen captures will not be marked as Alerts in **Viewer** as well).
4. Create a unique name for the created Alert and enter a description to this Alert in the **Description** field, if necessary.
5. Click **Browse** to select hosts to which the Alert will be applied.
6. The **Host Assigning** window appears.

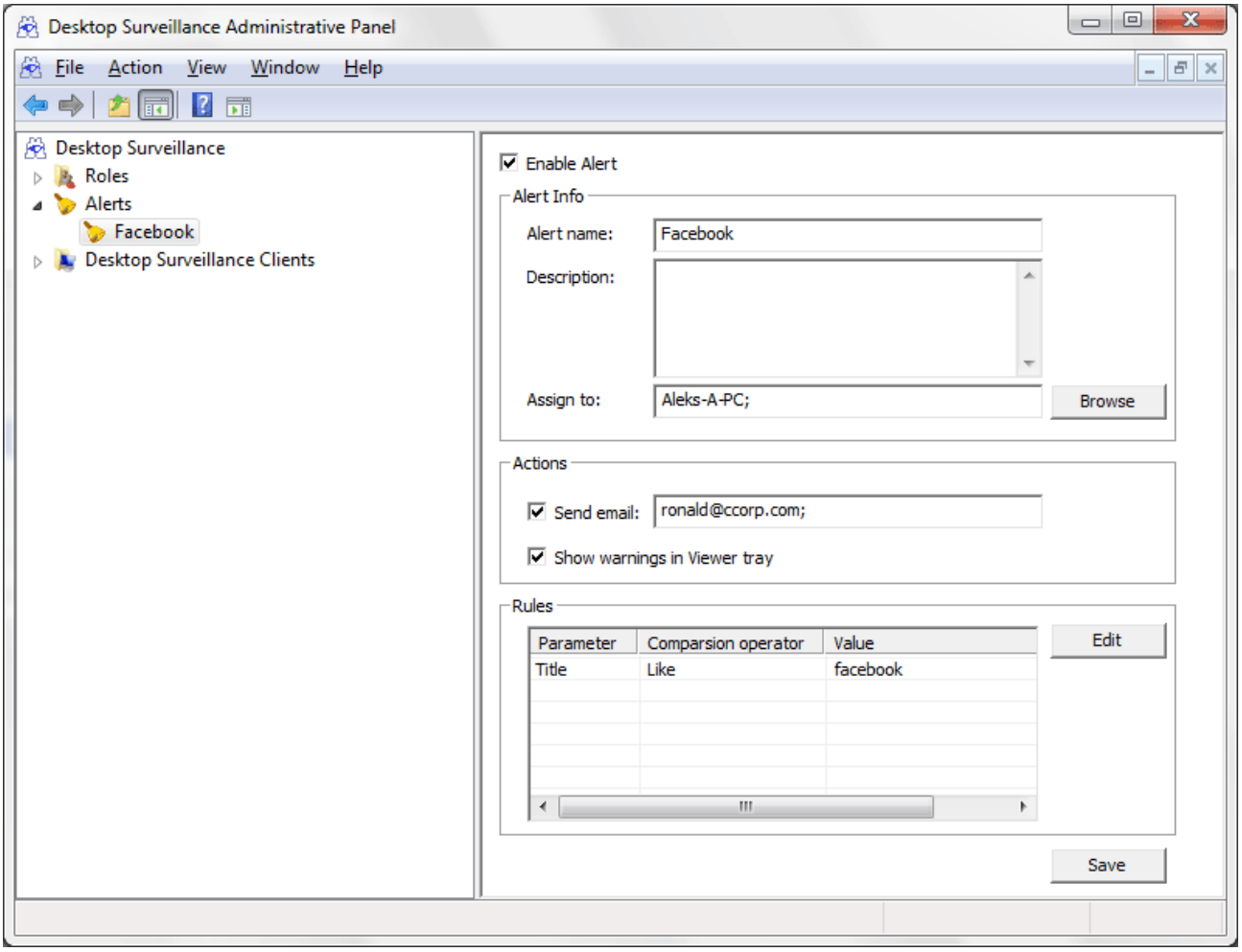
7. Check the check boxes near the target clients. Click **Check all** to apply the Alert to all clients. Click **Uncheck all** to clear all check boxes.

8. To receive email notifications on alert events, check the **Send email** check box and enter the email address to which the notifications will be sent. You can enter several email addresses, separating them with semicolon.

9. Check the **Show warnings in Viewer tray** check box to activate the tray notifications. The Alert notifications will then pop up from the tray on all computers with started **Viewer**.

10. In the **Rules** group, click **Edit** to define the rules for the created Alert. At least one rule has to be defined.

11. Click **Save** to save the changes.



Rules

Alert rules allow the investigator to determine what events on the investigated computer will be considered alert. Each alert has to have at least one rule. Rules applied to one parameter are combined with OR logic, rules applied to different parameters are combined with AND logic.

Rules are displayed in the grid in the **Rules** group in the **Alerts editing pane**.

Each rule consists of the **Parameter**, **Comparison Operator** and **Value**, to which the **Parameter** will be compared.

To edit the rules, click the **Edit** in the **Alert editing pane**, the **Rules** window appears.

To define a new rule, in the **Rules** window, do the following:

1. Select **Application**, **Title** or **Name** from the **Parameter** drop-down list.
2. Select the **Comparison operator** for the selected **Parameter**.
3. Enter the **Value**.

To delete a rule, clear the **Value** field in the **Rules** window.

The following parameters are available for the rules

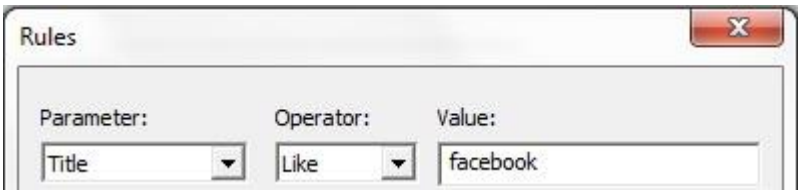
Parameter	Description	Example
Application	The name of the started application on the investigated computer. Set this parameter type for Alert to be activated whenever the specified value is identified as the name of a launched application.	skype.exe
Title	The name that appears in the title of a window. Set this parameter type for Alert to be activated whenever the specified value is identified in any title on the screen.	Facebook
User name	The name of the Windows user whose work is monitored by CensorNet Desktop Surveillance. Set this parameter type for Alert to be activated whenever the specified user uses the computer on which the Client is installed.	John

Comparison operators for text data:

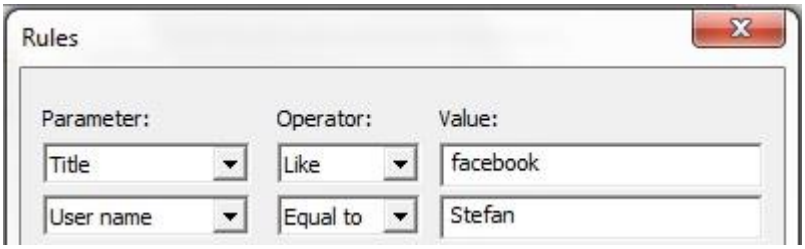
- **Equal to**: The defined value fully corresponds to the found result (e.g., John will find John, but will not find Johny);
- **Like**: The found result includes the defined value (e.g., John will find Johny, Johnatan, but will not find Johan);

Examples of Rules

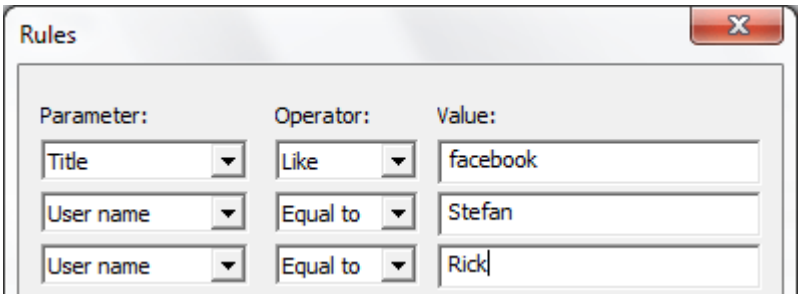
1. To set up the alert notification about any user opening **Facebook** on the investigated computer, enter the following parameters:



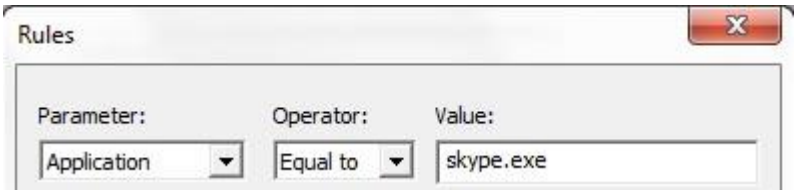
2. To set up the alert notification about a specific user (e.g. Stefan) opening **Facebook** on the investigated computer, enter the following parameters:



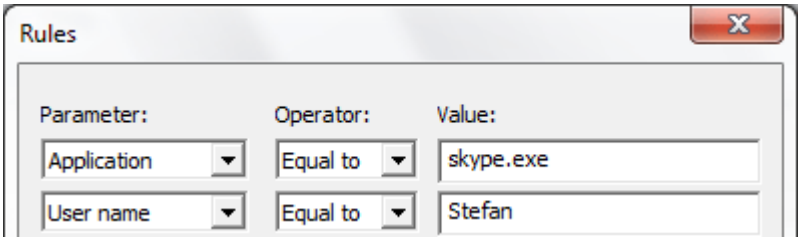
If you enter more than one name, the alert notification will then appear if any of them (Stefan or Rick) opens **Facebook**.



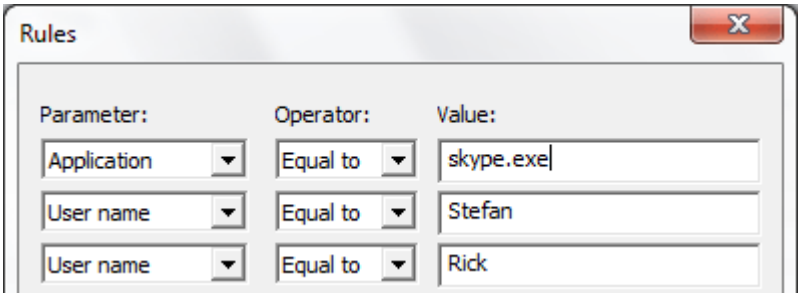
3. To set up the alert notification about any user launching **skype.exe** application on the investigated computer, enter the following parameters:



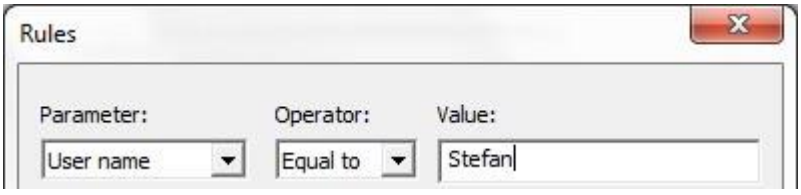
4. To set up the alert notification about a specific user (e.g. Stefan) launching **skype.exe** application on the investigated computer, enter the following parameters:



If you enter more than one name, the alert notification will then appear if any of them (Stefan or Rick) launches **skype.exe**.



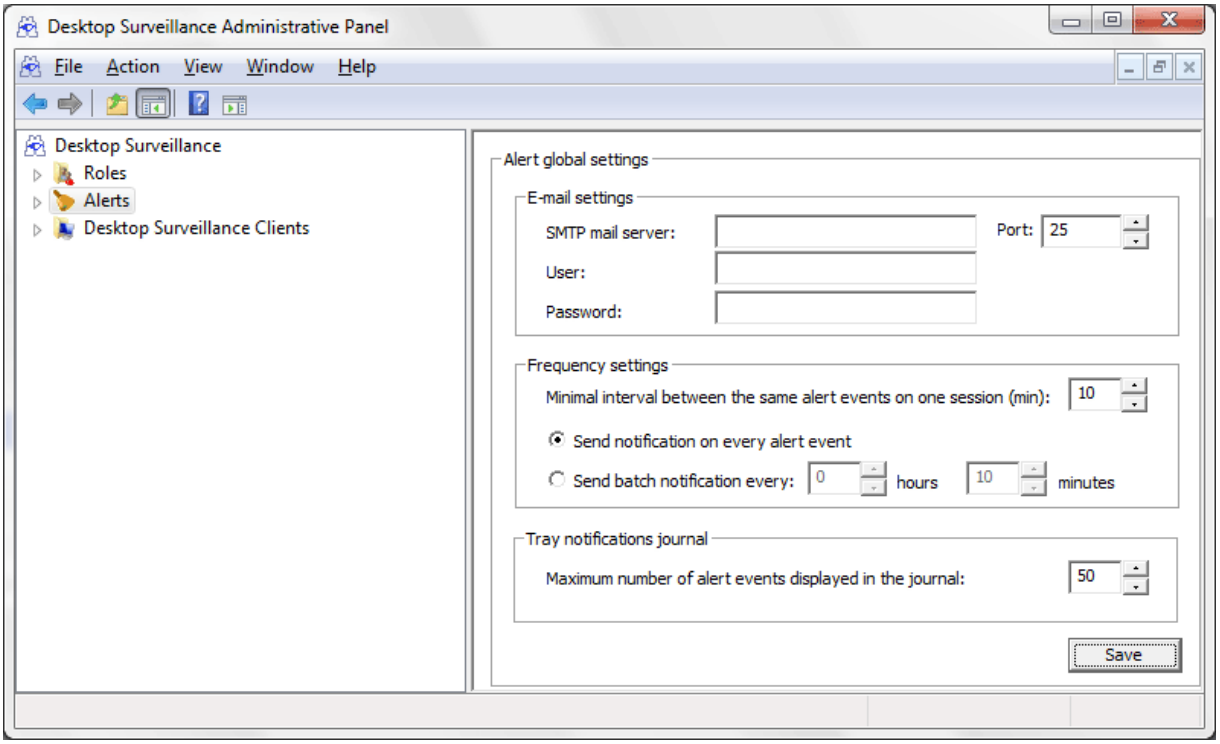
5. To set up the alert notification about a specific user (e.g. Stefan) using the investigated computer, enter the following parameters



Defining Alert Global Settings

Alert Global Settings define notification settings for all Alerts. These settings are applied to all Alert and to all **Desktop Surveillance Viewers** connected to this **Server**.

To define Alerts Global Settings, click the Alerts node. The **Alert global settings** pane will appear.



The **E-mail settings** group allows you to define a sender of the email alert notifications.

- Define an existing **SMTP mail server**.
  NOTE: The delivery of email notifications via mail servers with only NTLM authentication, such as Microsoft Exchange Server, is not supported.
- Define the number of the **Port** via which the emails will be sent.
- Define the login details (**User** and **Password**) of an existing email account, from which the email notifications will be sent.

The **Frequency settings** group allows you to define how frequently the Alert notifications will appear in the **Viewer Tray** and be sent via email.

1. Define the **Minimal interval between notifications sent for the same alert event**. This option defines how frequently the notifications about the same alert event will appear. For example, if this parameter is set to 10 minutes and a user has started Skype and works in it, the investigator will receive one notification every 10 minutes instead of receiving 10 notifications every minute or even more.
2. Define the way in which the notifications will be sent:

- Select **Send notifications on every alert event** for the notification on every alert event to be sent to the investigator.
- Select **Send batch notification every** for information on all alert events during defined time interval to be sent to the investigator.
- If **Send batch notification every** is selected, then define time interval in **hours** and **minutes**. Time counting starts when **Server** starts if this option is selected. Notifications are then sent with the defined frequency.

The **Tray Notifications Journal** group contains only one parameter that allows the investigator to define the maximum number of events displayed in the **Tray Notification Journal**. When it is reached, the oldest records are removed from the journal of all **Desktop Surveillance Viewers** (but not from the database).

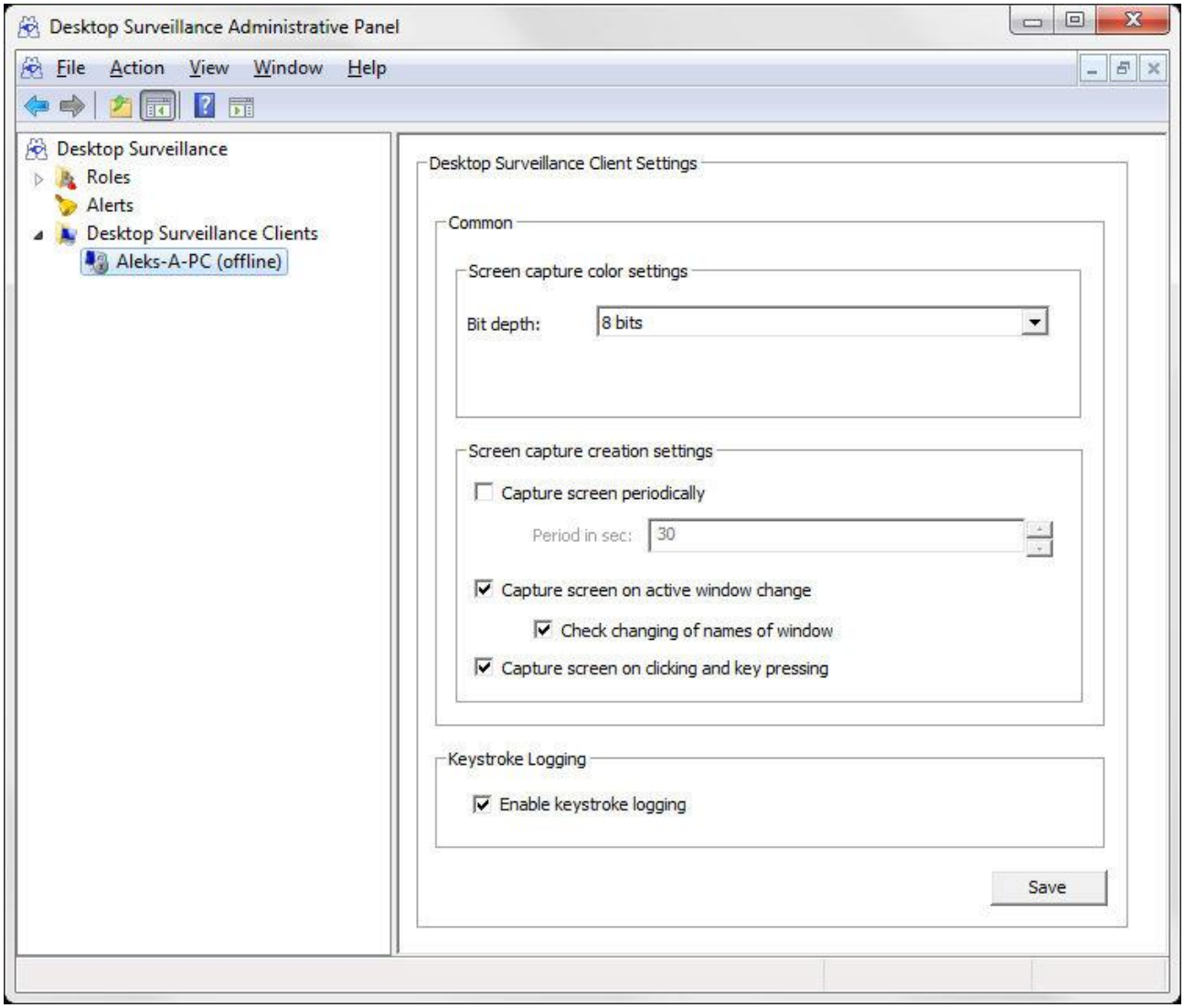
Desktop Surveillance Client Configuration

Hosts are computers on which CensorNet Desktop Surveillance Client installed. After the Client is installed on the computer it appears in the Hosts list of the Administrative Panel to which it connects.

Desktop Surveillance Client configuration is defined during installation or after the installation through editing the Desktop Surveillance Client configuration.

To edit the Desktop Surveillance Client configuration:

1. Select the required host under Desktop Surveillance Clients.
2. The configuration options are displayed in the Details pane.



3. Define the required screen capture quality. This option allows you to define the color depth of the created screen captures.
4. Define the screen captures creation frequency. This option allows you to define how often the screen captures on the Client computer will be created. Screen captures can be created by three parameters:
    - **Capture screen periodically:** Screen captures will be created with a certain time interval. Irrespective to whether something changes on the screen or not.

- **Capture screen on active window change**: Screen captures will be created on the change of the active window. For example, a new window opens (program starts), a new tab in the browser opens, any secondary window opens, etc.
- **Check changing of names of window:** Screen captures will be created on the change of the name of the active window (influences the keystroke logging as well).
- **Capture screen on clicking and key pressing:** Screen captures will be created on each mouse click or keyboard key pressing.

5. Define whether the keystroke logging must be enabled by selecting the **Enable keystroke logging** checkbox.
   NOTE: The keystrokes are not logged in a virtual machine session. To log keystrokes from a virtual machine session, you need to install a Client on the virtual machine.
6. Click **Save**.
7. A new configuration will be immediately applied to the host.

Export

CensorNet Desktop Surveillance Administrative Panel allows you to export the list of roles and/or hosts to the *.txt and *.csv format.

To export data:

1. In the Navigation pane, expand the category to be exported, e.g., Hosts (to export the lists of all hosts connected to the Administrative Panel) or Administrator (to export the list of all Windows users to whom the Administrator role is assigned).
2. Select **Action > Export List** or right-click and select **Export List**.
3. Select the name of the file to which data is to be exported and its format.
4. Data is exported.

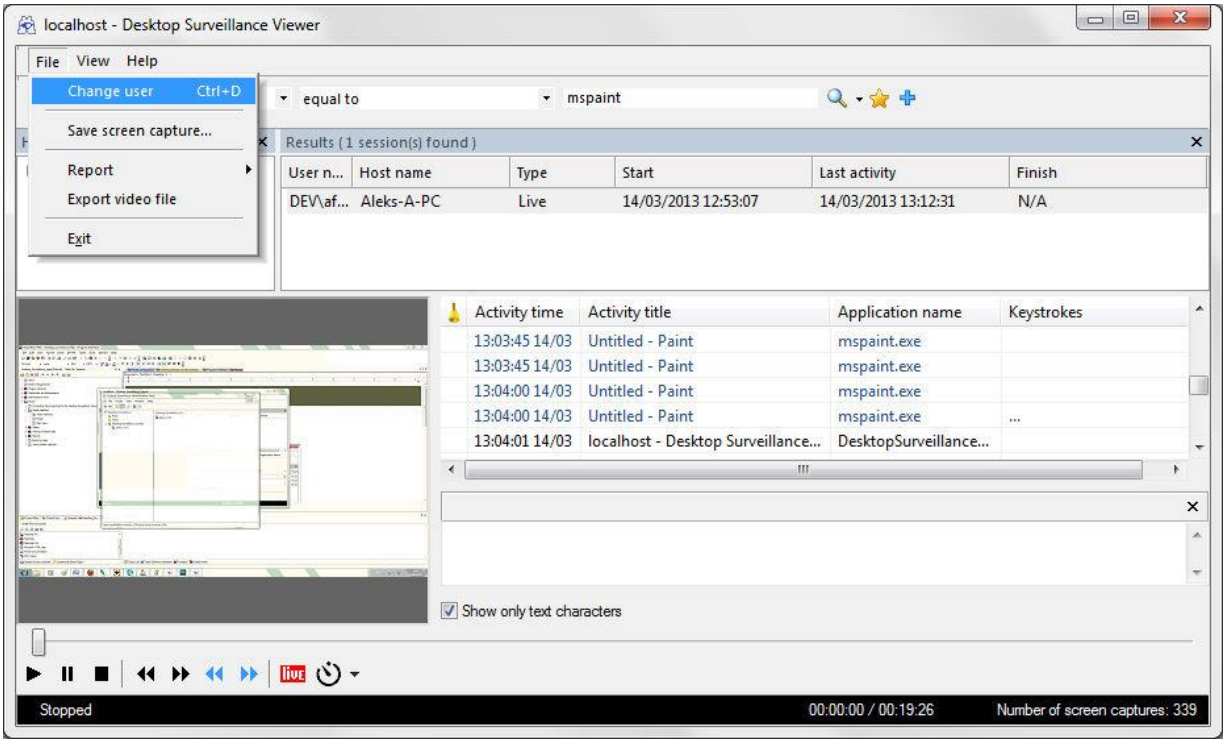
Viewer

Connecting/Disconnecting from Desktop Surveillance Server

Disconnecting from the Desktop Surveillance allows you to change the user. Only users, to which **Administrator** or **Auditor** roles are assigned in the **Desktop Surveillance Administrative Panel** (part of the Desktop Surveillance Server), can connect to the **Desktop Surveillance Viewer**.

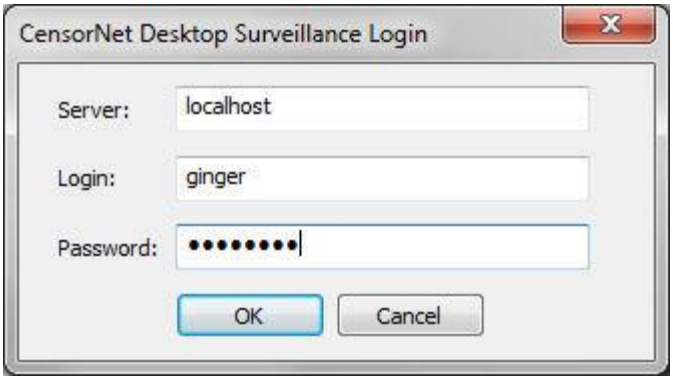
To change the user, do the following:

1. In the main menu, select **File - Change user** or press **Ctrl + D**.



2. The **CensorNet Desktop Surveillance Login** window opens. Enter the following parameters and click **OK**:
    - **Server:** Enter the server name. It can be the IP address, name, or localhost (if the server is installed on the local computer).
    - **Login:** Enter the login name. It can be **<username>** if it is the local user and **<domainname\username>** if the user is added to the domain.

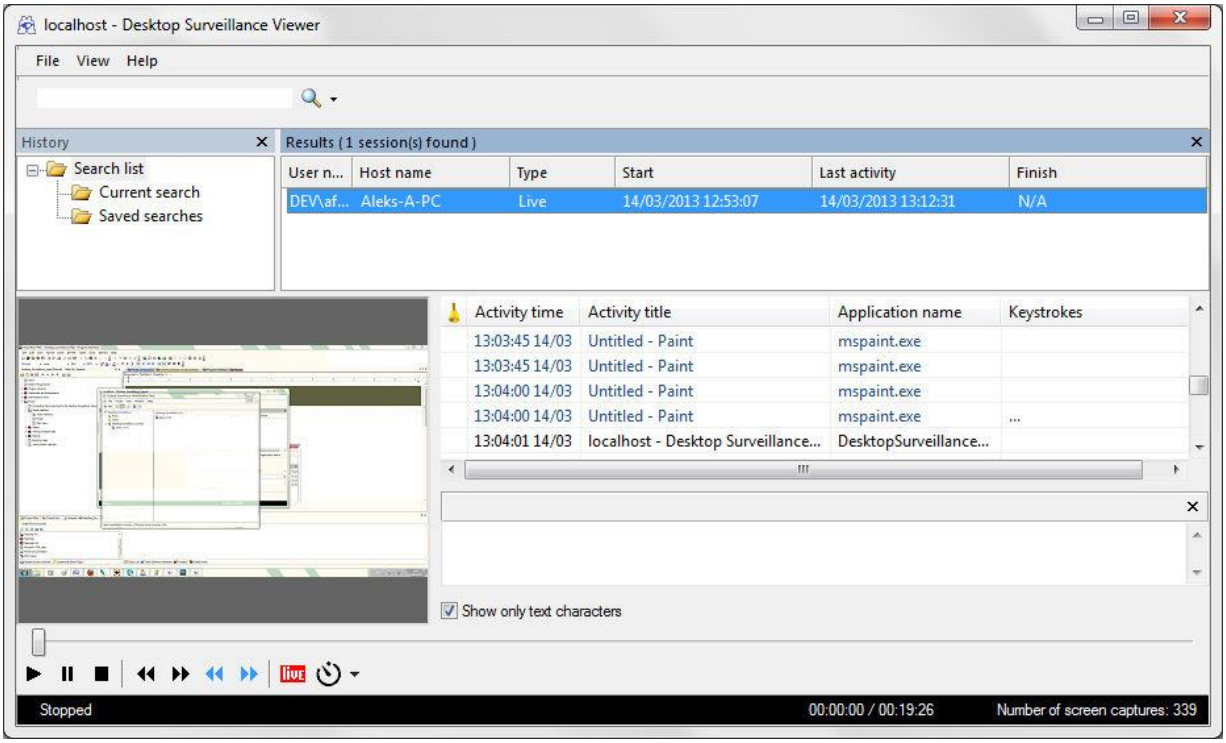
      NOTE: If there is no network connection, you need to enter the login name as follows: <name of the computer>\<username>
    - **Password:** Enter the Windows user password.



3. The user is changed and connected to the CensorNet Desktop Surveillance.

Viewer interface

Viewer Interface


localhost - Desktop Surveillance Viewer
File View Help
History
Search list
Current search
Saved searches
Results (1 session(s) found)
User n... Host name Type Start Last activity Finish
DEV\af... Aleks-A-PC Live 14/03/2013 12:53:07 14/03/2013 13:12:31 N/A
Activity time Activity title Application name Keystrokes
13:03:45 14/03 Untitled - Paint mspaint.exe
13:03:45 14/03 Untitled - Paint mspaint.exe
13:04:00 14/03 Untitled - Paint mspaint.exe
13:04:00 14/03 Untitled - Paint mspaint.exe
13:04:01 14/03 localhost - Desktop Surveillance... DesktopSurveillance...
Show only text characters
Stopped
00:00:00 / 00:19:26
Number of screen captures: 339

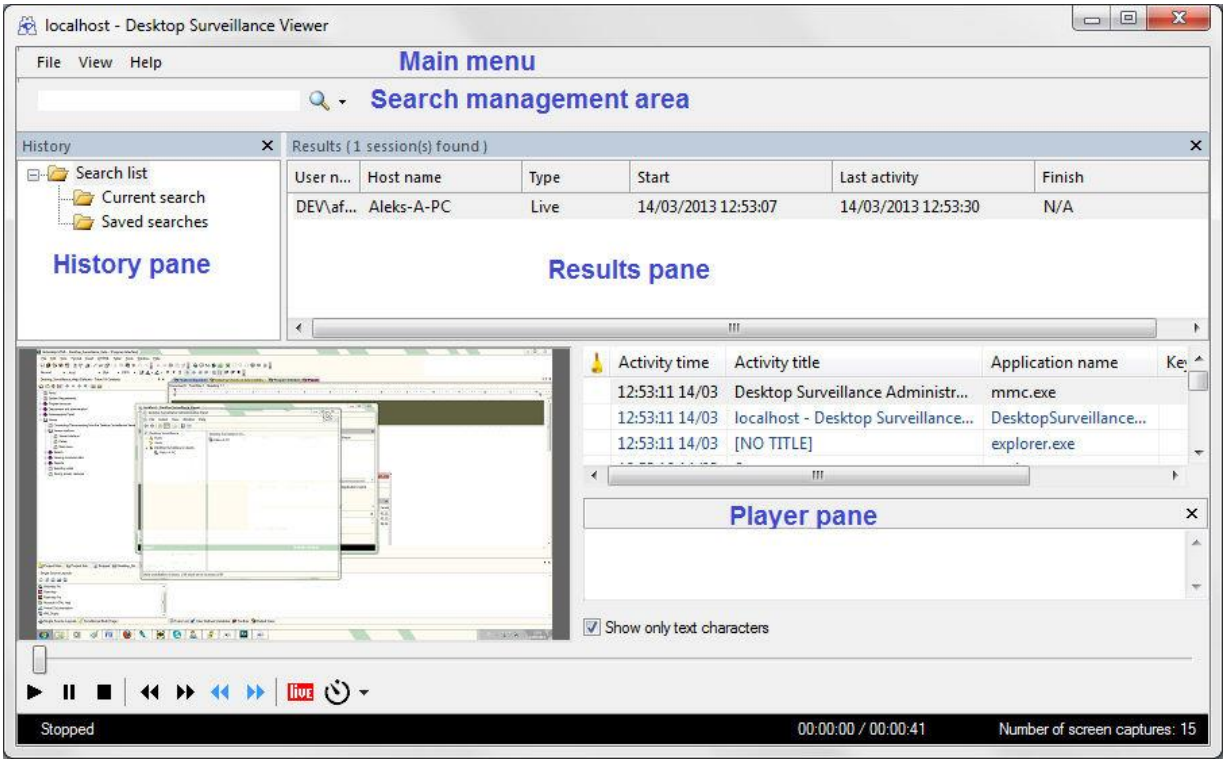
By default, the **Desktop Surveillance Viewer** interface is divided into the following areas:

- The **Main menu**: Provides you the access to the features of the **Desktop Surveillance Viewer** program.
- The **Search management area**: Allows you to perform quick and parameterized searches.
- The **History pane**: In this pane, the current and favorite searches are displayed.
- The **Results pane**: In this pane, the detailed results of the search are displayed.
- The **Player pane**: In this pane, the list of screen captures and the player window are displayed.

Panes

The **Desktop Surveillance Viewer** interface consists of five main areas:

- **Search management area**
- **History pane**
- **Results pane**
- **Player pane**



The Search management area

This area includes parameters for the search in the Desktop Surveillance sessions.

The History pane

In this pane, the **Search list** tree-view structure is displayed:

- **Current search**: This folder contains the parameters and results of the current search.
- **Saved searches**: This folder contains the **saved user search parameters**.

The Results pane

In this pane, the search results are displayed. The search results fields are filled when the search finishes. The results are displayed in a grid with the following columns:

- **User name**: The name of the Desktop Surveillance user.
- **Host name**: The name of the computer on which the Client is installed.
- **Type**: The search type. It can be **Finished**, **Live**, and **Non-Licensed**.
- **Start**: The date when the session started.
- **Last activity**: The date of the last made screen capture.
- **Finish**: The date when the session finished. If the session has the **Live** status, this field is empty.

The Player pane

The Player pane is divided into two areas: the list of screen captures (to the right) and the player itself (to the left).

The list of screen captures is displayed in a grid with the following columns:

- **Alert icon:** If the screen capture matches the alert criteria, an alert icon, representing a bell, will be displayed here.
- **Activity time**: The date and time when the screen capture was made.
- **Activity title**: The name that is associated with the screen capture.
- **Application name**: The name of the application that was started on the Client computer.
- **Keystrokes:** The content of the keystrokes log associated with the selected screenshot.
  NOTE: The keystrokes are not logged in a virtual machine session. To log keystrokes from a virtual machine session, you need to install a Client on the virtual machine.

You can change the size of the columns. Data is sorted by the time of the screen capture creation.

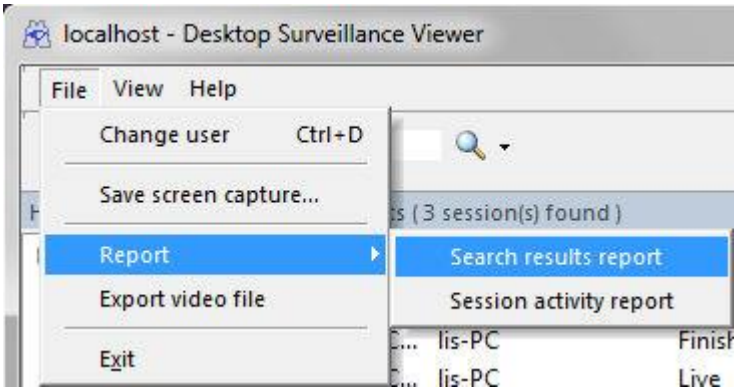
Main Menu

The main menu of the Desktop Surveillance Viewer provides the access to the features of the program.

The main menu consists of three parts:

- **File menu**
- **View menu**
- **Help menu**

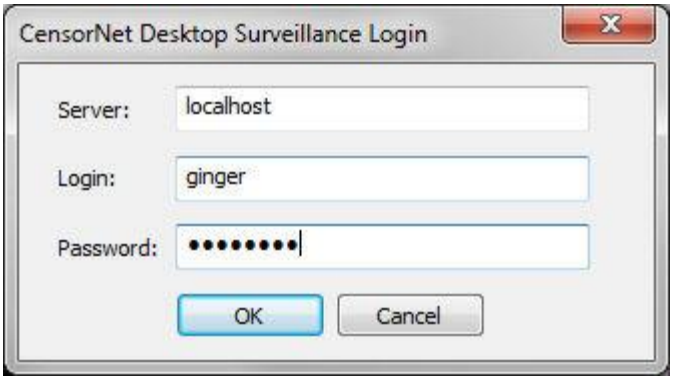
File menu



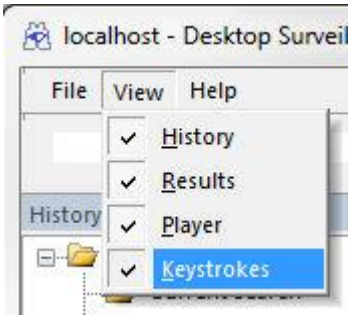
The File menu consists of four options:

- **Change user**: Allows you to change the Desktop Surveillance Viewer user.
- **Save screen capture**: Allows you to save the selected screen capture to a file.
- **Report**: Allows you to generate two types of reports.
- **Export video file**: Allows you to export the screen captures from the session to a video file format.
- **Exit**: Allows you to exit the Desktop Surveillance Viewer.

When disconnecting from the Desktop Surveillance Server, the **CensorNet Desktop Surveillance Login** window opens. Fill the **Login** and **Password** fields and click **OK** to connect to the CensorNet Desktop Surveillance Server.



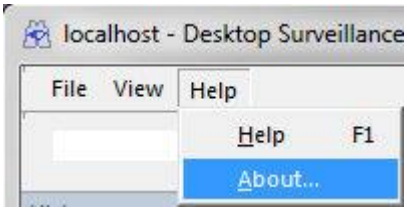
View menu



The View menu consists of four options that allows you to enable/disable panes:

- **History**: Allows you to enable/disable the History pane.
- **Results**: Allows you to enable/disable the Results pane.
- **Player**: Allows you to enable/disable the Player pane.
- **Keystrokes:** Allows you to enable/disable the keystrokes displayed in the Player pane.

Help menu



The Help menu consists of two options:

- **Help**: Provides you the access to this help file.
- **About**: Provides you with information about the Desktop Surveillance Viewer application.

Search

About Searching

You can perform searches in the **CensorNet Desktop Surveillance** sessions. Each session contains a set of screen captures made from the investigated computer during the specified period of time. You can search by the following parameters: name of the screen capture, the application name, user, name of the computer

with installed Client, date of the session start, date of the session finish, date of the last made screen capture, and type of the session.

There are two types of searching:

- **Quick:** Allows you to perform searching by the text data.
- **Parameterized:** Allows you to perform searching using multiple parameters.

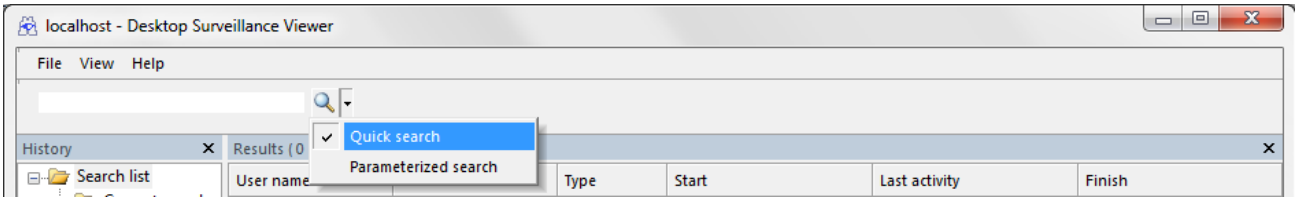
Quick Search

The quick search allows the investigator to perform searches by the text data, i.e. by the name of the application, the screen capture title, user name, host name, and the type of the session.

The quick search is enabled by default.

To perform a quick search, do the following:

1. In the **Search management area** (under the **Main menu**), click on the arrow near the **Search** button and select **Quick search**.



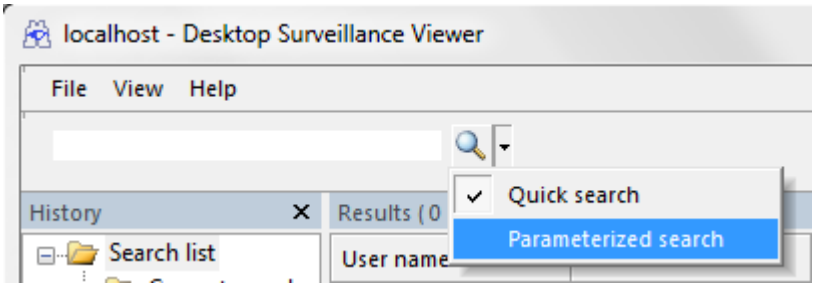
2. In the **Search** field, enter the required data by which you want to perform searching.
3. Click on the **Search** button or press **Enter**.
4. The search starts.
5. When the search finishes, the results are displayed in the **Results pane**.
6. Click the session in the **Results pane** to view the detailed information in the **Player pane**.

Parameterized Search

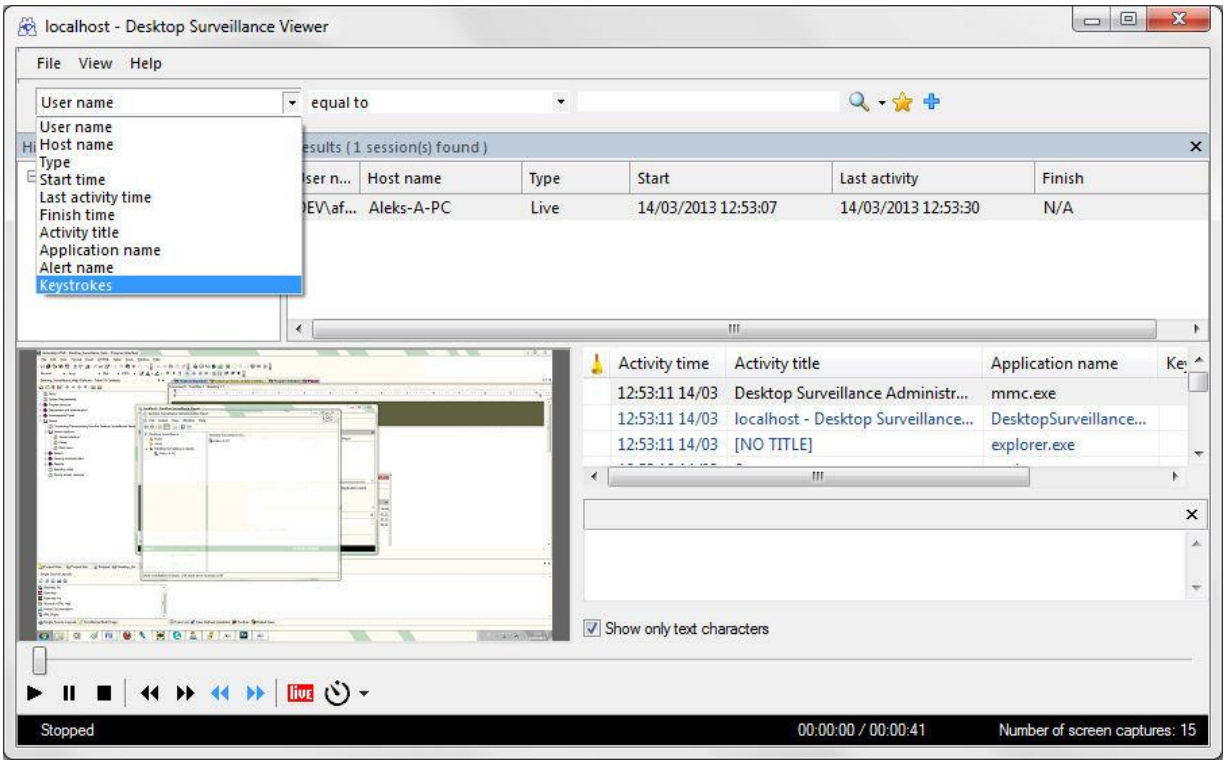
The parameterized search allows the investigator to perform searching in the Desktop Surveillance sessions using multiple parameters.

To perform a parameterized search, do the following:

1. In the **Search management area** (under the **Main menu**), click on the arrow near the **Search** button and select **Parameterized search**.



2. The **parameterized search area** opens.



3. By default, there is only one search condition. To add another condition, click on the plus button. The new condition line will be displayed below the first one.

   NOTE: Search conditions of different types are connected with "AND" logic. Search conditions of the same type are connected with "OR" logic.

4. Define the search parameters.
5. When adding the **Start**, **Finish time**, or **Last Activity time** condition, the **Now** option is available. Select this option to perform the search till the current computer date.
6. Click on the **Search** button or press **Enter**.
7. The search starts. When the process of searching finishes, the results are displayed in the **Results pane**.

Parameterized Search Parameters

The **parameterized search condition** consists of the **Parameter** box, **Comparison operator** box, and the **Value** box.

You can add up to 10 conditions. **To add the condition**, click the plus icon. **To delete the condition**, click on the minus icon. The conditions of different types are connected with "**AND**" logic, it means that each specified condition will be TRUE for each found session in the Results pane. The conditions of the same

type are connected with **"OR"** logic, it means that at least one of the specified conditions of the same type will be TRUE for each found session in the Results pane.

Text data parameters

Search Item	Description	Example
User name	The name of the Windows user whose work is monitored by CensorNet Desktop Surveillance.	John
Host name	The name of the computer on which the Client is installed.	Kenny
Type	The type of the session. The following types are available: Finished (the session is finished), Live (the session is running), Non-Licensed (the computer with the Client has no license).	Finished, Live
Activity title	The name associated with the screen capture. It associates with the currently opened window on the investigated computer, context menu, etc.	Start menu
Application name	The name of the started application on the investigated computer.	explorer.exe
Alert name	The name of the alert that occurred on the investigated computer.	Facebook alert
Keystrokes	A phrase or a word that was logged on the investigated computer.	Corporate security

Comparison operators for text data:

- **equal to**: the defined value fully corresponds to the found result (e.g., John will find John, but will not find Johny);
- **like**: the found result includes the defined value (e.g., John will find Johny, Johnatan, but will not find Johan);

Date parameters

Search Item	Comparison Operator	Example

Start time	The date of the session start.	9/13/2010
Last Activity time	The date of the last made screen capture.	12/13/2009
Finish time	The date of the session finish.	12/12/2008

Additional options:

- **Now**: Select this option to enable the searching till the current date.

Comparison operators for dates:

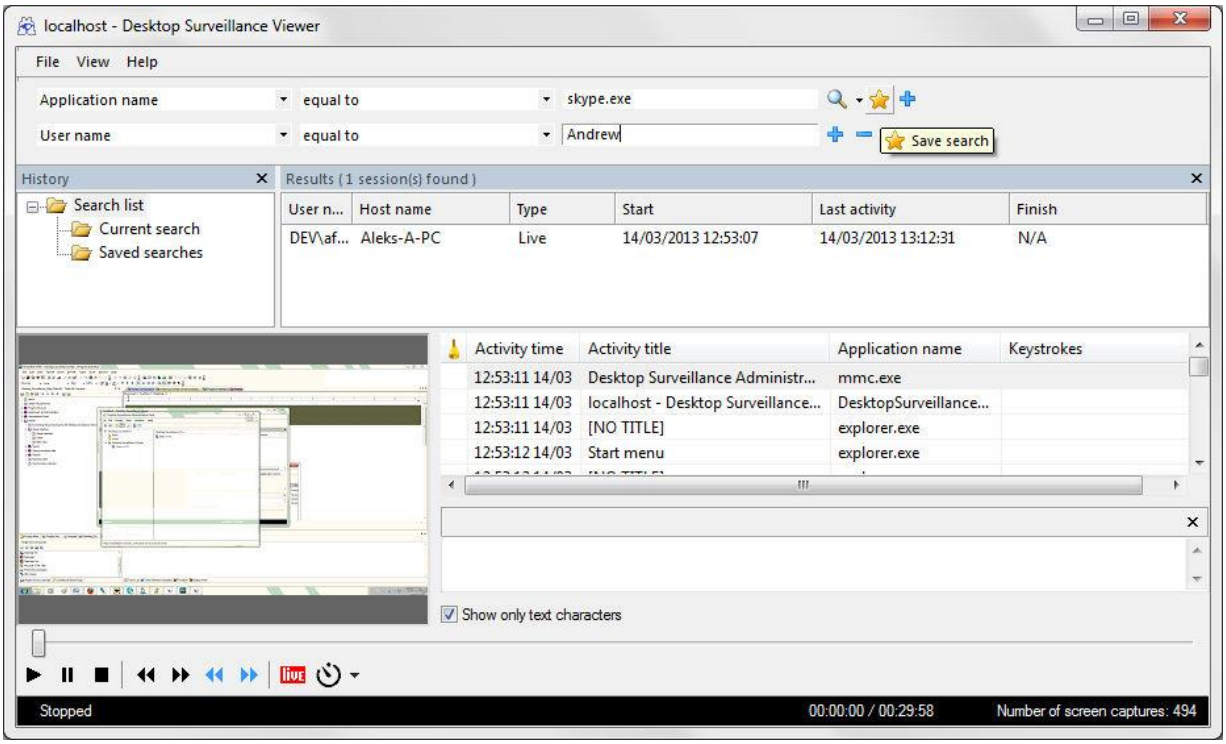
- **equal to**: the specified date fully corresponds to the found result (e.g., 12/12/2009 will find 12/12/2009 but will not find 12/11/2009);
- **before**: the found results will match all the dates till the specified one (e.g., 12/12/2009 will find 07/08/2009 but will not find 12/12/2010);
- **after**: the found results will match all dates after the specified one (e.g., 12/12/2009 will find 12/12/2010 but will not find 12/12/2008).

Saving Search Parameters

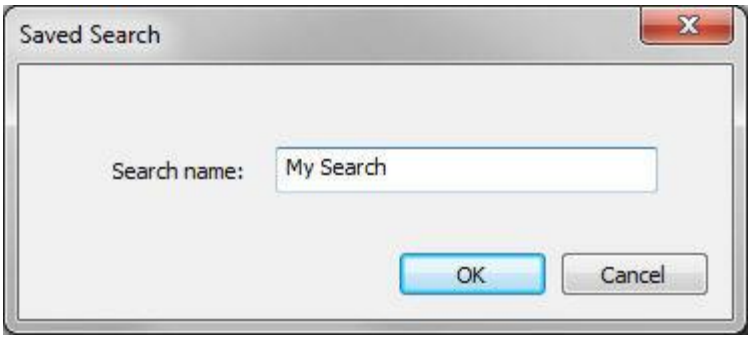
You can save the search parameters to make it easier to perform further searches. The search parameters will be saved in the **Saved searches** folder in the **History** pane. The saving of search parameters is available only for the **parameterized search**.

To save the search parameters, do the following:

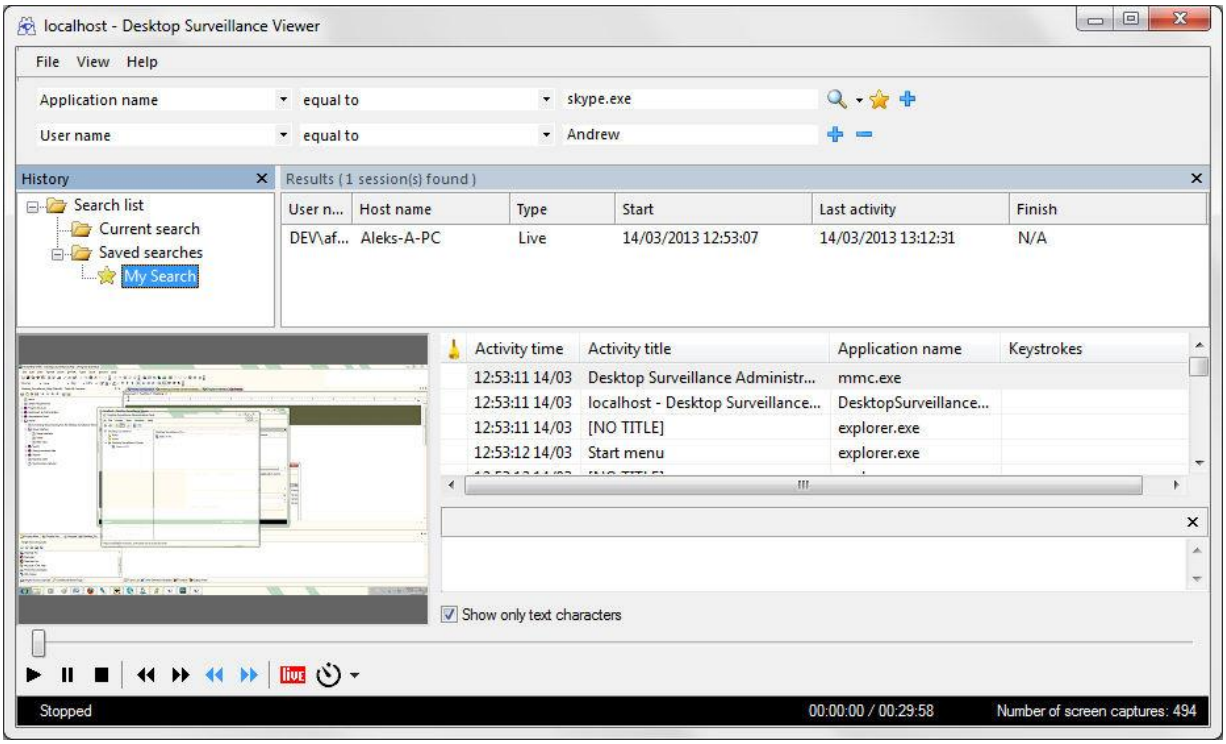
1. Define the search parameters.



2. Click the **Save search** icon.
3. The **Saved Search** window opens.
4. Enter the name for the set of the search parameters and click **OK**.



5. The search parameters are added to the **Saved searches** folder. You can view it in the **History pane**.



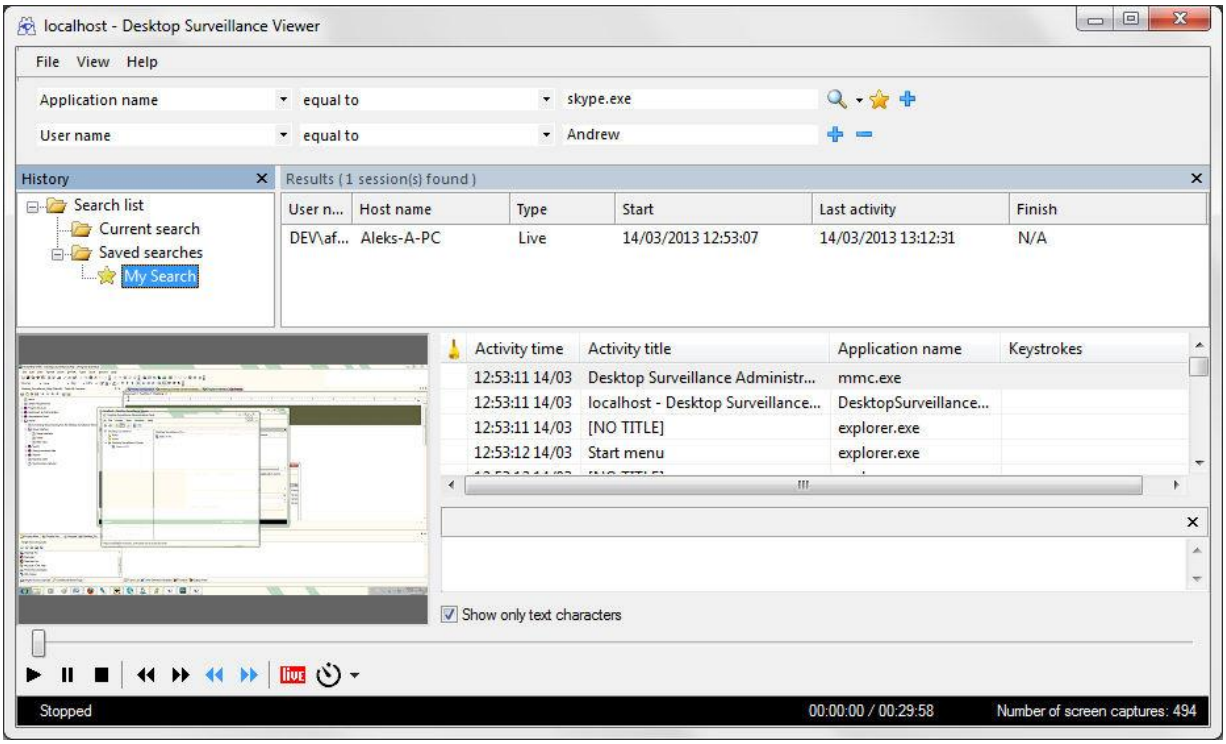
NOTE: When opening search parameters that include dates (Finish time, Start, or Last activity time) with enabled Now option, the date will be set as the current one.

Restoring Search Parameters

You can restore the saved search parameters. This makes it easier to perform further searches without defining the same parameters again.

To restore the search parameters, do the following:

1. In the **History pane**, navigate to the **Saved searches** folder in the **Search list** tree.
2. In the **Saved searches** folder, select the required folder with saved search parameters.

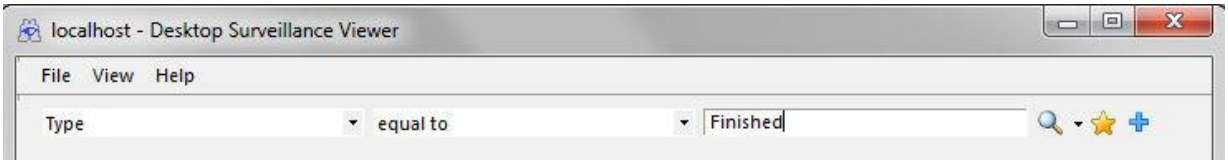


3. The saved search parameters are displayed in the **Search management area**.
4. Click the search button or press **Enter** to start searching.

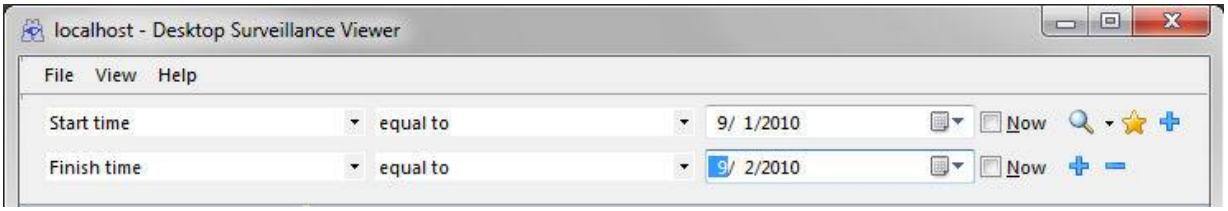
Examples of Search Parameters

1. To find all screen captures connected with the work of **explorer.exe**, enter the following parameters:

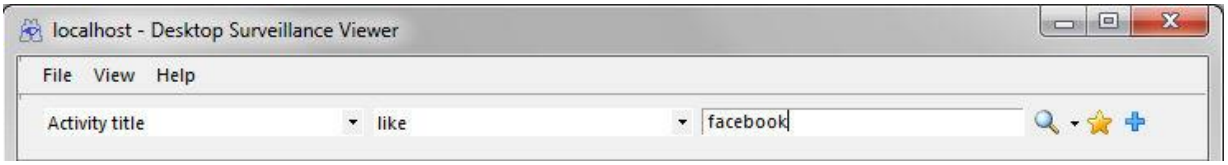
2. To find all **finished** Desktop Surveillance sessions, enter the following parameters:



3. To find all sessions started on **September 1, 2010** and finished on **September 2 2010**, enter the following parameters:



4. To find all sessions connected with **Facebook**, enter the following parameters:



5. To find all sessions connected with the discussion of **corporate policy**, enter the following parameters:

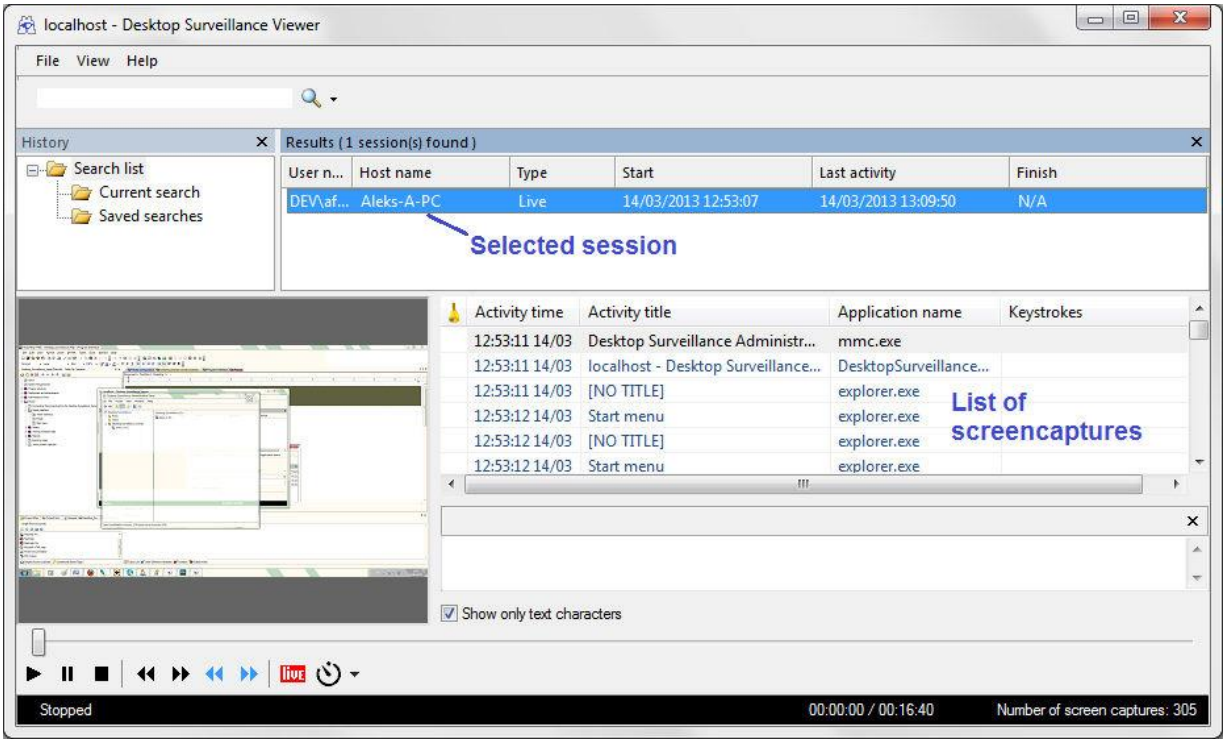
Viewing monitored data

Viewing Screen Captures

The Desktop Surveillance Viewer allows you to view the screen captures made from the computer on which the Client is installed. You can view them separately by selecting the required screen capture from the list or viewing all screen captures in the form of video.

To view the screen captures, do the following:

1. In the **Results pane**, select the required session.
2. The list of all screen captures from the session are displayed in the form of grid in the right part of the **Player pane**.



3. The Player is not playing by default. Do one of the following:
   - In the list of screen captures, select the required screen capture. It is displayed in the **Player area**.

- In the list of screen captures, select the screen capture starting from which you want the video to be streamed. In the **Player area**, click **Play**. Screen captures are displayed in order one by one.

To pause/stop the video, use the corresponding **Pause** and **Stop** control buttons in the **Player area**.

To move from one screen capture to the next one, use the **Previous/Next** control buttons.

To move to the full-screen mode, double click the screen capture in the **Player area**.

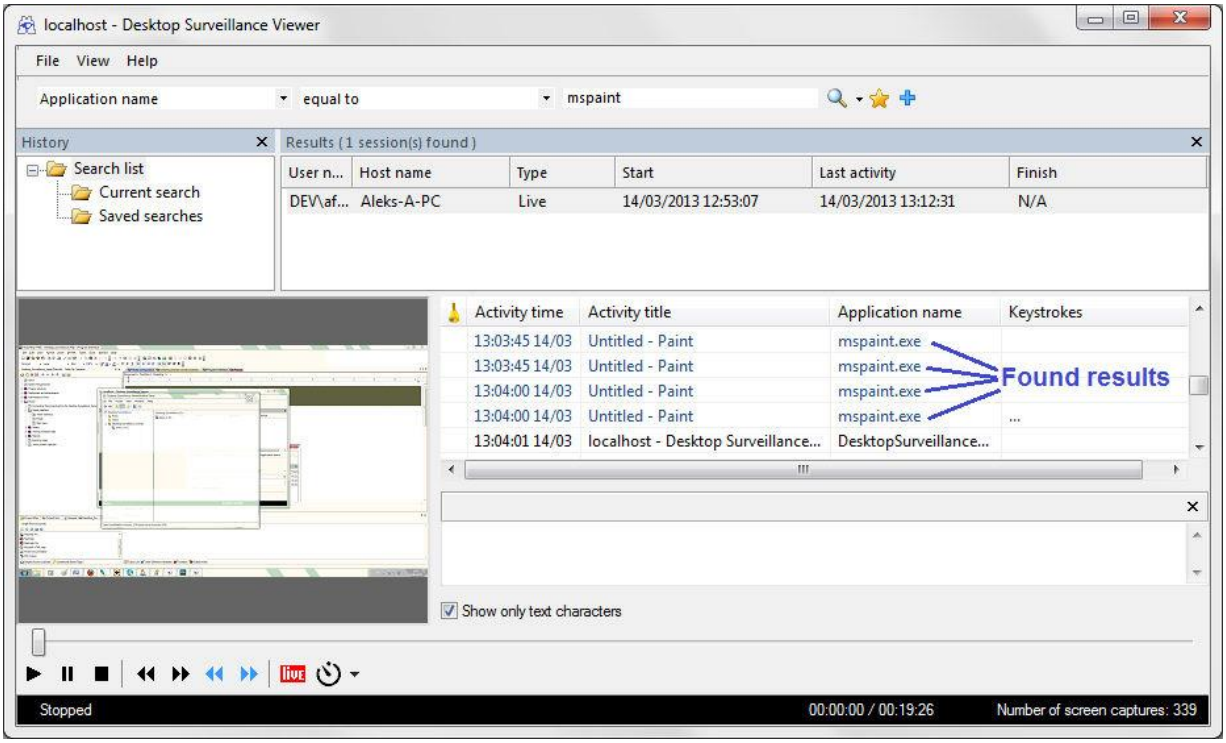
You can define the speed with which screen captures will change in the **Player area**. To do this, click **Video speed** and in the drop-down list, select **Actual** to change screen captures depending on the screen capture creation time; select **1 fps** to display one screen capture per second.

If the search conditions included the **Title** and **Application** items, the additional control buttons are displayed in the **Player area**. They are marked blue and allow moving between the found search results.

When you select a screen capture, the keystrokes associated with it are displayed in the box, below the list of screen captures. By default it displays only text characters, you can enable displaying all keystrokes logged (e.g. navigation buttons, functions keys, etc.) by clearing the **Show only text characters** checkbox. Then any other keys and key combinations will be displayed in inequality sign brackets. If a key was pressed repeatedly it will be displayed with an "x" sign and the number of reiterations (e.g. <F12 x 24>).

Please note that keystrokes are not logged from virtual machines.

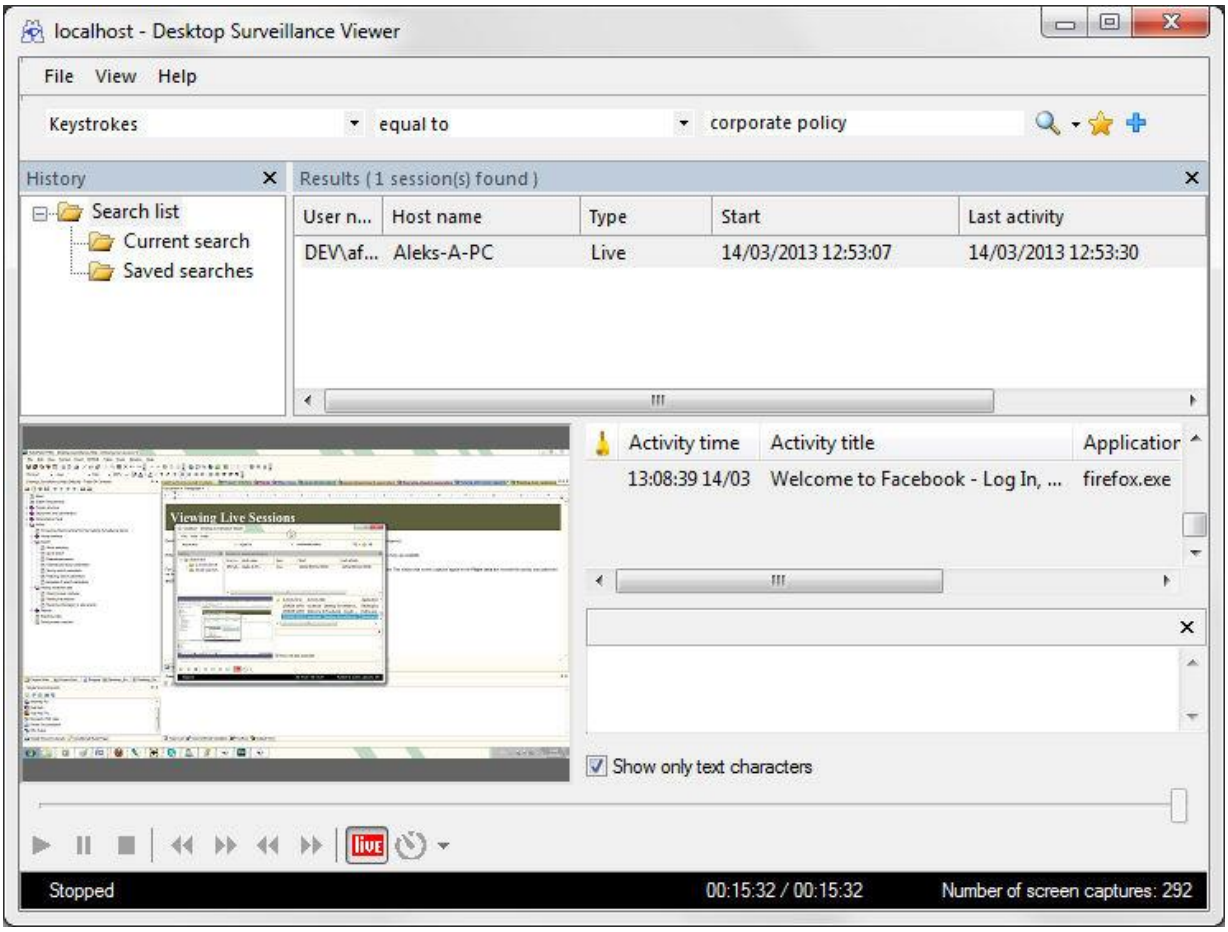
NOTE: If the Enter key was pressed during input, the log will be split in the list of screen captures. Though to maintain text integrity, in the keystrokes box, the keystrokes lines having the same Title-Application pair will be put together.



Viewing Live Sessions

Desktop Surveillance Viewer allows you to view screen captures in a Live session (i.e., the monitoring of the Client computer is still in progress).

If the session has the **Live** status, the list of screen captures is refreshed each second and new screen captures are added to the table if any are available.



For Live sessions, the additional button is available in the **Player area**. When you click this button, the real-time monitoring is performed. This means that screen captures appear in the **Player area** the moment the activity was performed on the investigated computer.

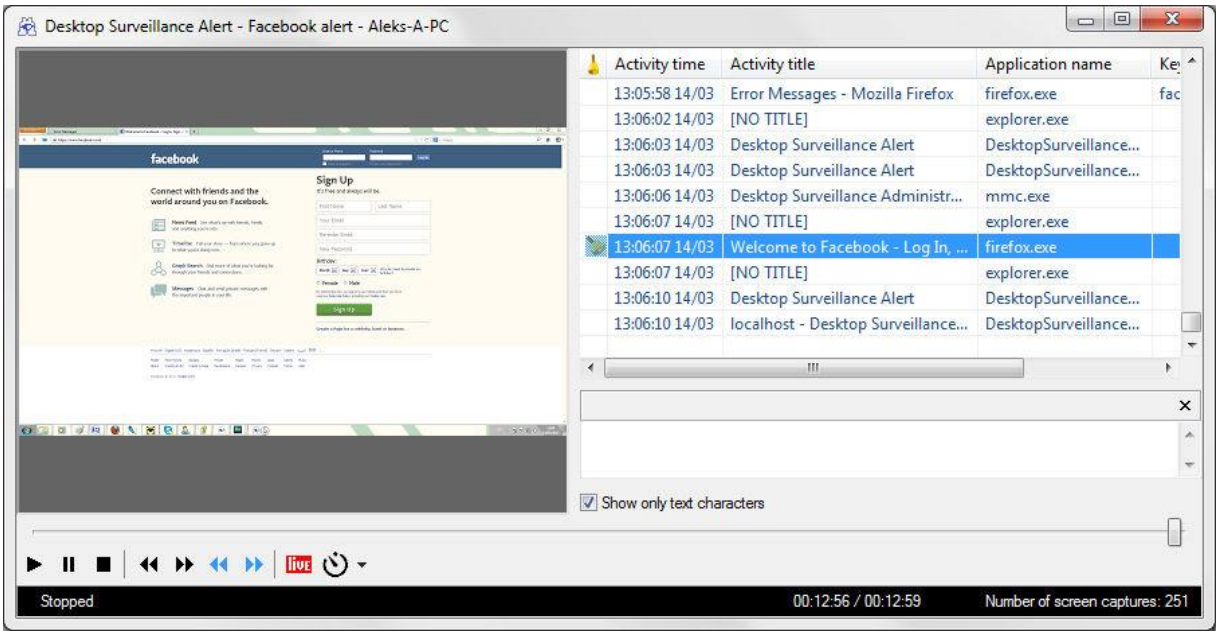
NOTE: If you click this button, you will not be able to navigate between screen captures in the list.

Receiving Information on Alert Events

The investigator can receive information on Alert events in three ways:

- In the **Viewer** application, when the investigator browses the screen captures. The alert events are marked with a special icon.
- If email notifications are enabled in the **Alert Parameters**, the alert information can be received in the email alert notification that also contains the link for viewing this alert in the **DesktopSurveillance Viewer**.

  NOTE: You need the Viewer to be properly installed in order to activate links in the email notifications.
- If the tray notifications are enabled in the **Alert Parameters**, the information can be displayed by clicking the **View in the Desktop Surveillance Viewer** link in the pop-up notification from the **Viewer Tray**. Or this information can be received from the **Tray Notifications Journal** called from the **Viewer Tray** context menu.


Desktop Surveillance Alert - Facebook alert - Aleks-A-PC
Activity time
Activity title
Application name
13:05:58 14/03 Error Messages - Mozilla Firefox firefox.exe
13:06:02 14/03 [NO TITLE] explorer.exe
13:06:03 14/03 Desktop Surveillance Alert DesktopSurveillance...
13:06:03 14/03 Desktop Surveillance Alert DesktopSurveillance...
13:06:06 14/03 Desktop Surveillance Administr... mmc.exe
13:06:07 14/03 [NO TITLE] explorer.exe
13:06:07 14/03 Welcome to Facebook - Log In, ... firefox.exe
13:06:07 14/03 [NO TITLE] explorer.exe
13:06:10 14/03 Desktop Surveillance Alert DesktopSurveillance...
13:06:10 14/03 localhost - Desktop Surveillance... DesktopSurveillance...
Show only text characters
Stopped
00:12:56 / 00:12:59
Number of screen captures: 251

Reports

About Reports

The investigator can generate a report to export search results to a separate file. The report is generated in the *.xls format.

The following two types of reports are available:

- Search Results report: This type of report includes information on all found sessions. The following data is included: number of found sessions, search type, date of the report generation, types of sessions, host names, activity time, and number of screen captures. Report can also include detailed information on each found session.
- Session Activity report: This type of report includes information on the user activity in one or more sessions.

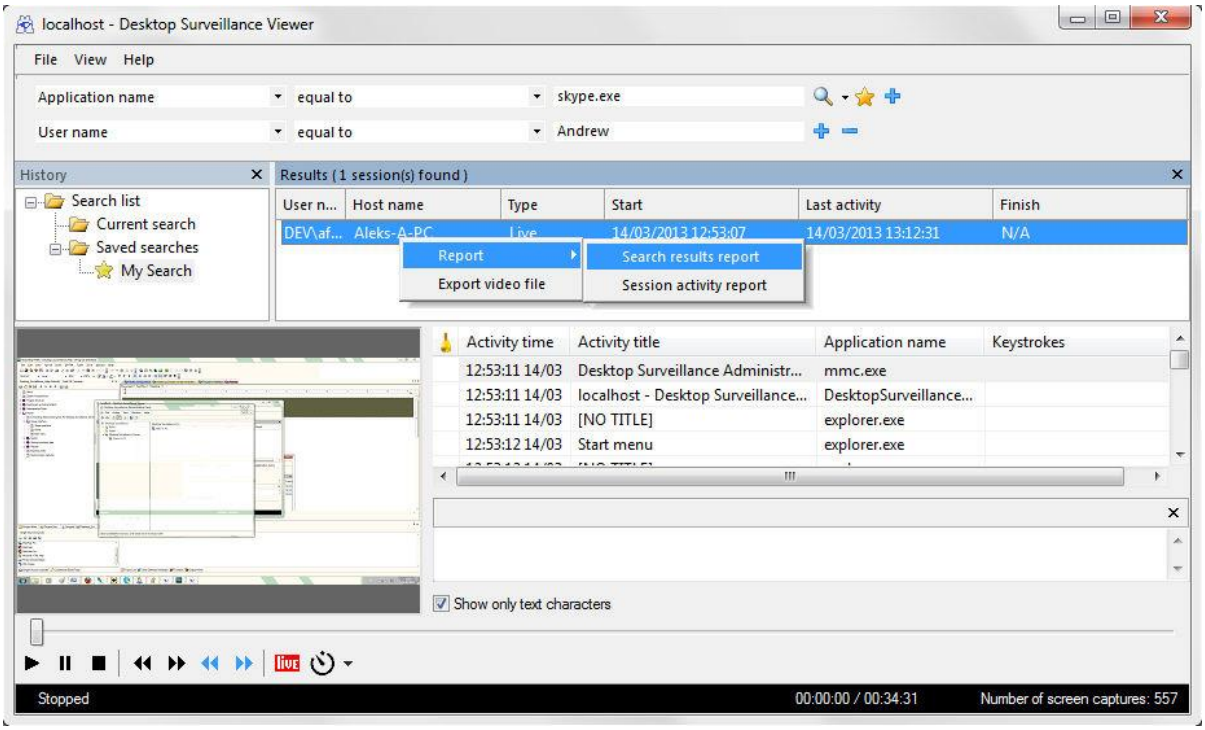
Search Results Report

Search Results report includes information on all found sessions. The following information is included to the report: date of report generation, path to the report, type of the search, number of found sessions, types of sessions (live or finished), names of the investigated computers, activity time, etc. If the investigator used parameterized search, search parameters and their values are also included to the report.

The report can also include detailed information for each found session. Information on each session is displayed in a separate tab named **<number>Session**. It includes general information on the session and the table with the names of screen captures and their creation date and time as it is displayed in the list of screen captures in the **Player pane**.

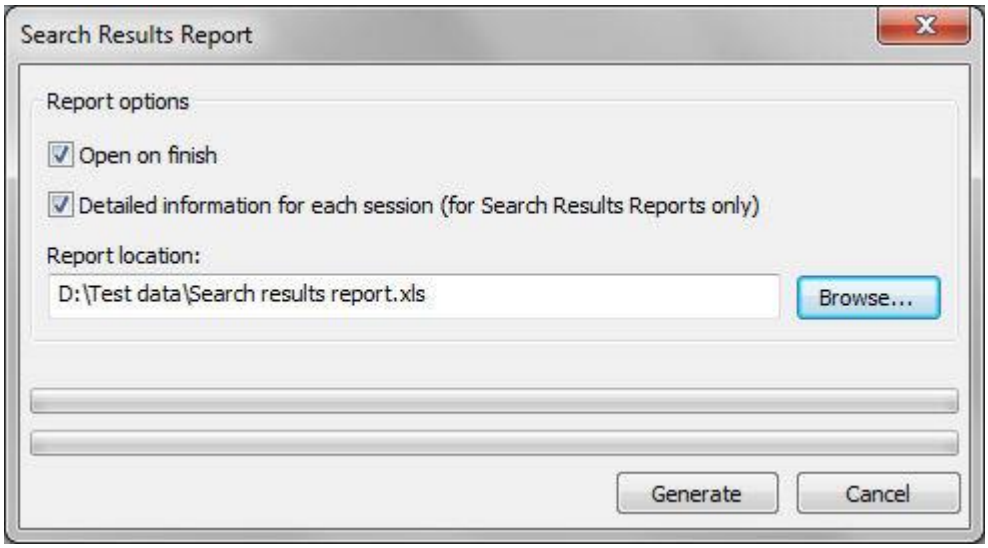
To generate the Search Results report, do the following:

1. In the main menu, select **File - Report - Search Results Report** or right click the session in the **Results pane** and select **Report - Search Results Report**.



NOTE: The report can be generated for more than one session. Multi-selection is available in the Results pane.

2. The **Search Results Report** window opens.



3. In the **Report Options**, select the required options. The following options are available:
    - **Open on finish**: Select this option to automatically open the report after the generation process finishes.
    - **Detailed information for each session (for Search Results Reports only)**: Select this option to include detailed information for each session to the report.
4. In the **Report location** field, do one of the following:
    - Enter the path to the generated report manually.
    - Click **Browse** and define the location for the file with generated report.
5. Click **Generate** to generate the report.
6. When the generation process finishes, click **Finish**. The report will open automatically if the corresponding option was selected.

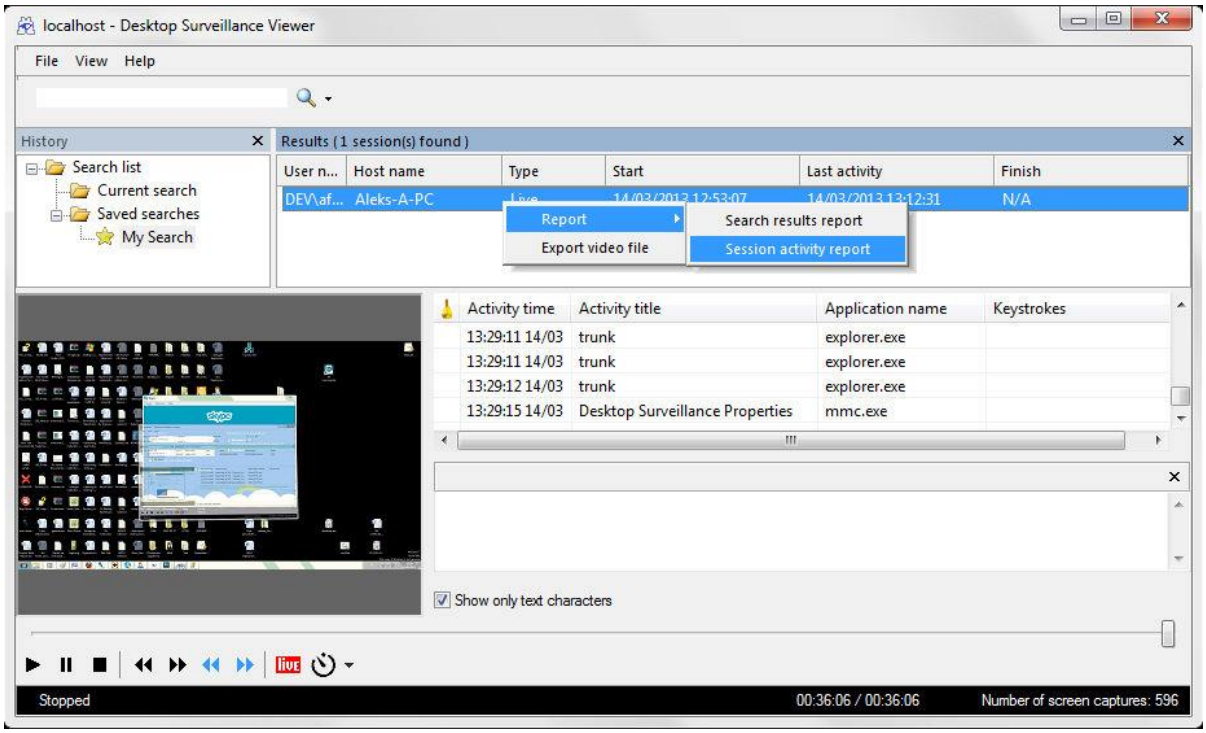
Session Activity Report

The Session Activity report includes general information on the user activity in the session currently opened in the Player pane. Also, detailed information on the session activity is displayed in a separate tab named **<hostname><date and time of the session start>**.

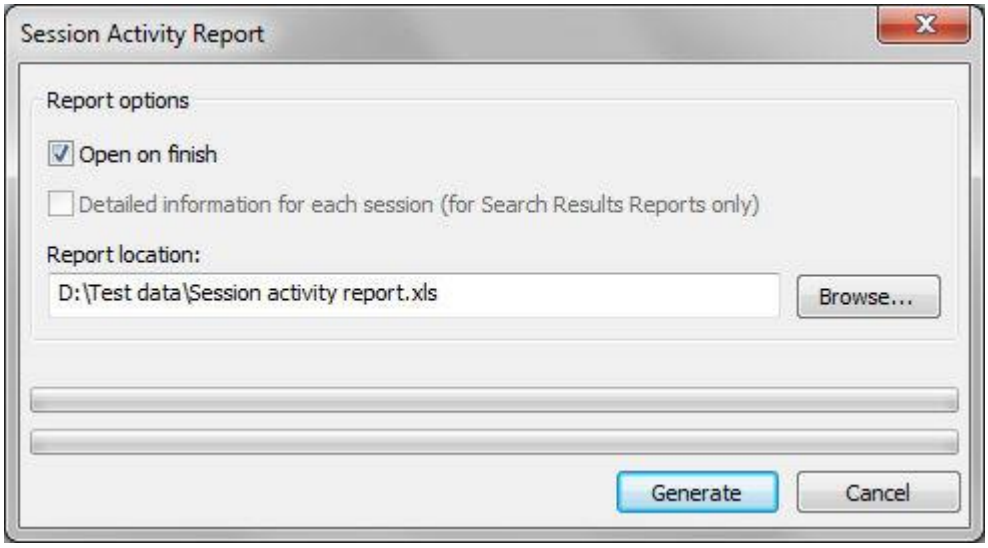
> **NOTE: The investigator can use Ctrl and Shift keys to select more than one session in the Results pane. In this case, report will include detailed information on each selected session.**

To generate the Session Activity report, do the following:

1. In the main menu, select **File - Report - Session Activity Report**.



2. The **Session Activity Report** window opens.



3. Select the **Open on finish** option to automatically open the report after the generation process finishes.
4. In the **Report location** box, do one of the following:
    - Enter the path to the generated report manually.
    - Click **Browse** and define the location for the file with generated report.
5. Click **Generate** to generate the report.
6. When the generation process finishes, click **Finish**. The report will open automatically if the corresponding option was selected.

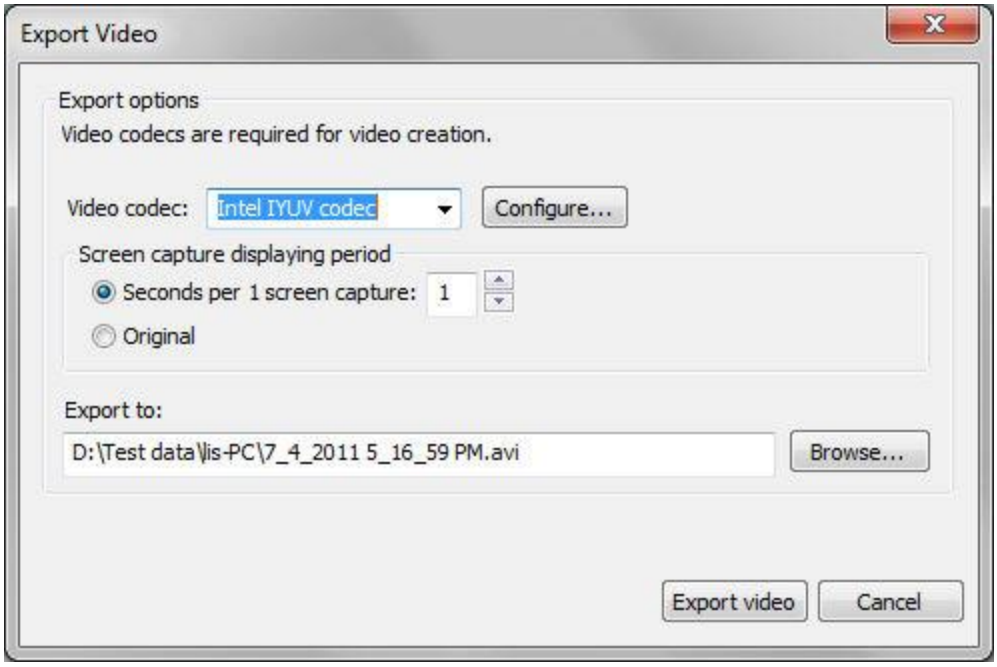
Exporting Video

Exporting video means exporting screen captures of the session in the video format to your computer. Video is exported in the *.avi format. Video resolution will be the same as the resolution of screen captures received from the Client computer.

To export video, do the following:

1. In the main menu, select **File - Export video file**, or right click the session in the **Results pane** and select **Export video file**, or right click the **Player Management panel** and select **Export video file**.

   NOTE: You can export the whole session as well as a part of it. To select screen captures for exporting, use Ctrl and Shift keys.
2. The **Export Video** window opens.



3. In the **Video codec** drop-down list, select the required codecs with the help of which video will be created. Please note that the list contains only the system codecs that will be used for video creation.
4. Click **Configure** to configure the selected codec. Configuration window depends on the selected codec.
5. In the **Screen capture displaying period** group of options, select the speed with which video will play. The following options are available:

- **Seconds per 1 screen capture**: Define the time interval in seconds with which screen captures will change in the video file.
- **Original**: Video will play with a real speed depending on the frequency of created screen captures.

6. In the **Export to** field, do one of the following:
   - Enter the path to the video file manually.
   - Click **Browse** and navigate to the location fro the exported video file.
7. Click **Export video** to export the session.
8. When the export process finishes, click **Finish**.
9. Navigate to the folder with exported data.

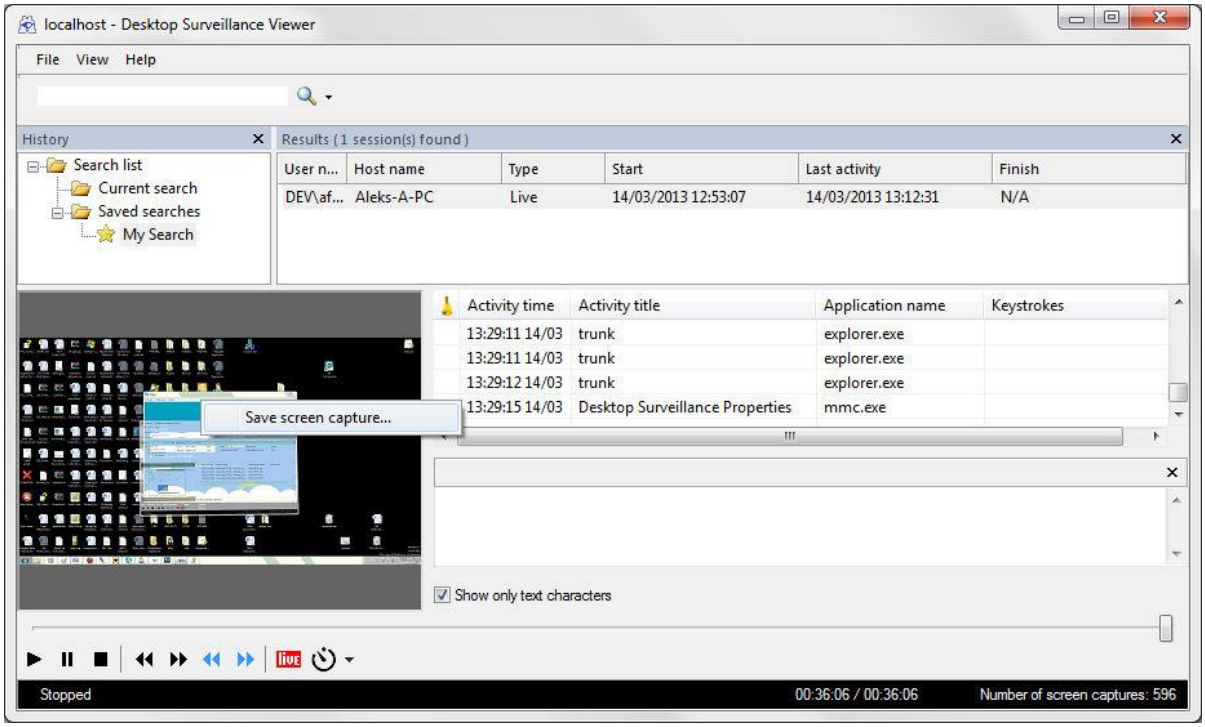
   NOTE: If there was a change of resolution on the Client computer display or change of bit depth, several video files can be exported.

Saving Screen Captures

You can save the required screen capture to a file on your computer. Screen captures are saved in the *.png format.

To save the screen capture, do the following:

1. In the **Player pane**, in the list of screen captures, select the required screen capture.


localhost - Desktop Surveillance Viewer
File View Help
History
Search list
Current search
Saved searches
My Search
Results (1 session(s) found)
User n... Host name Type Start Last activity Finish
DEV\af... Aleks-A-PC Live 14/03/2013 12:53:07 14/03/2013 13:12:31 N/A
Activity time Activity title Application name Keystrokes
13:29:11 14/03 trunk explorer.exe
13:29:11 14/03 trunk explorer.exe
13:29:12 14/03 trunk explorer.exe
13:29:15 14/03 Desktop Surveillance Properties mmc.exe
Save screen capture...
Show only text characters
Stopped
00:36:06 / 00:36:06
Number of screen captures: 596

2. It is displayed in the **Player** window.
3. Right click the screen capture and select **Save screen capture** or in the main menu, select **File - Save screen capture**.
4. In the **Save As** window, define the name and location for the screen capture. Click **Save**.
5. The screen capture is saved.
6. Navigate to the folder with screen capture.

NOTE: You cannot save the screen capture if the video is playing or if there is a full-screen mode.